J.W. Price
949/261-8433
Makoto Tatebayashi et al.

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

NAK1-BI69

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: １９９８年１０月１６日

出 願 番 号
Application Number: 平成１０年特許願第２９５９２０号

出 願 人
Applicant (s): 松下電器産業株式会社

CERTIFIED COPY OF PRIORITY DOCUMENT

１９９９年１０月 １日

特 許 庁 長 官
Commissioner,
Patent Office

近 藤 隆 彦

【書類名】　特許願

【整理番号】　2022500408

【提出日】　平成10年10月16日

【あて先】　特許庁長官　　殿

【国際特許分類】　G09C　1/00

【発明の名称】　デジタル著作物保護システム

【請求項の数】　17

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　館林　誠

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　中村　穣

【特許出願人】

【識別番号】　000005821

【氏名又は名称】　松下電器産業株式会社

【代理人】

【識別番号】　100090446

【弁理士】

【氏名又は名称】　中島　司朗

【代理人】

【識別番号】　100109210

【弁理士】

【氏名又は名称】　新居　広守

【手数料の表示】

【予納台帳番号】　014823

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9810105

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　デジタル著作物保護システム

【特許請求の範囲】

【請求項１】　記録媒体とアクセス装置とが接続された状態で、両者間で機器認証フェーズと著作物転送フェーズとを実行して著作物の正当者への配布を実現するデジタル著作物保護システムであって、

機器認証フェーズでは、記録媒体が所有する固有鍵をアクセス装置に秘密伝送し、アクセス装置が取得した固有鍵を用いて、機器認証を行い、

著作物転送フェーズでは、機器認証が成功した場合にのみ、アクセス装置が取得した固有鍵を用いて著作物を暗号化して記録媒体に転送し若しくは記録媒体から転送された著作物を復号する

ことを特徴とするデジタル著作物保護システム。

【請求項２】　記録媒体とアクセス装置とが接続された状態で、前記記録媒体と前記アクセス装置との間で機器認証と暗号化された著作物の転送とを行うデジタル著作物保護システムであって、

前記記録媒体は、

記録媒体毎に異なる固有鍵を予め記憶している固有鍵記憶領域と、

接続されたアクセス装置へ前記固有鍵を秘密伝送し、前記固有鍵を用いて前記アクセス装置との間で機器認証を行う第１認証手段と、

前記固有鍵を用いて暗号化される著作物を保持するための領域とを備え、

前記アクセス装置は、

記録媒体から秘密伝送された固有鍵を用いて、前記記録媒体との間で機器認証を行う第２認証手段と、

機器認証が成功した場合にのみ、前記機器認証を経て得た固有鍵を用いて著作物を暗号化して記録媒体に転送し若しくは記録媒体から転送された著作物を復号する転送手段とを備える

ことを特徴とするデジタル著作物保護システム。

【請求項３】　前記第１認証手段は、あらかじめ第１鍵を有し、前記第１鍵を用いて、前記固有鍵に第１暗号を施して暗号化固有鍵を生成して伝送し、

前記第２認証手段は、あらかじめ前記第１鍵を有し、前記第１鍵を用いて、前記伝送された暗号化固有鍵に、前記第１暗号の逆変換を行う第１復号を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器認証を行い、

前記転送手段は、前記復号固有鍵を用いて著作物の転送を行う

ことを特徴とする請求項２記載のデジタル著作物保護システム。

【請求項４】　前記第１認証手段は、第１鍵を基にして、公開鍵暗号方式の公開鍵決定アルゴリズムにより算出された公開鍵である第２鍵をあらかじめ有し、前記第２鍵を用いて、前記固有鍵に第１暗号を施して暗号化固有鍵を生成して伝送し、

前記第２認証手段は、あらかじめ前記第１鍵を有し、前記第１鍵を用いて、前記伝送された暗号化固有鍵に、前記第１暗号の逆変換を行う第１復号を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器認証を行い、

前記転送手段は、前記復号固有鍵を用いて著作物の転送を行う

ことを特徴とする請求項２記載のデジタル著作物保護システム。

【請求項５】　前記第１認証手段は、あらかじめ第１鍵を有し、前記第１鍵を用いて、前記固有鍵に回復型署名処理を施して署名文を生成して伝送し、

前記第２認証手段は、前記第１鍵に前記回復型署名処理の公開鍵決定アルゴリズムにより算出された公開鍵である第２鍵をあらかじめ有し、前記第２鍵を用いて、前記伝送された署名文に、前記回復型署名の検証処理を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器認証を行い、

前記転送手段は、前記復号固有鍵を用いて著作物の転送を行う

ことを特徴とする請求項２記載のデジタル著作物保護システム。

【請求項６】　前記デジタル著作物保護システムは、さらに

固有鍵に第１暗号を施して暗号化固有鍵に変換する固有鍵変換手段を備える暗号化固有鍵作成装置を有し、

前記第１認証手段は、前記固有鍵を前記固有鍵変換手段へ出力して暗号化固有鍵に変換し、変換された暗号化固有鍵を前記アクセス装置へ伝送し、

前記第２認証手段は、記録媒体から伝送された暗号化固有鍵に前記第１暗号の逆処理を行う第１復号を施して固有鍵を生成する

ことを特徴とする請求項２記載のデジタル著作物保護システム。

【請求項７】　前記第１認証手段は、あらかじめ複数の第１鍵を有し、前記複数の第１鍵のうち一つの第２鍵の選択を受け付け、前記第２鍵を用いて、前記固有鍵に第１暗号を施して暗号化固有鍵を生成して伝送し、

前記第２認証手段は、あらかじめ複数の第１鍵を有し、前記複数の第１鍵から前記第２鍵の選択を受け付け、前記第２鍵を用いて、前記伝送された暗号化固有鍵に、前記第１暗号の逆変換を行う第１復号を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器認証を行い、

前記転送手段は、前記復号固有鍵を用いて著作物の転送を行う

ことを特徴とする請求項２記載のデジタル著作物保護システム。

【請求項８】　アクセス装置と接続された状態で、前記アクセス装置との間で機器認証と暗号化された著作物の転送とを行う記録媒体であって、

記録媒体毎に異なる固有鍵を記憶している固有鍵記憶領域と、

前記固有鍵を用いて暗号化される著作物を保持するための領域と、

アクセス装置が接続されたとき、記録媒体から当該アクセス装置へ固有鍵を秘密伝送する手順を経て、当該アクセス装置との間で機器認証を行う認証手段と、

機器認証が成功した場合にのみ、前記固有鍵を用いて暗号化された著作物を受け取り前記領域に書き込み若しくは前記領域に記憶されている暗号化された著作物を読み出して前記アクセス装置へ出力する転送手段と

を備えることを特徴とする記録媒体。

【請求項９】　固有鍵を有する記録媒体と接続され、前記記録媒体との間で機器認証と暗号化された著作物の転送とを行うアクセス装置であって、

記録媒体から固有鍵を秘密伝送される手順を経て、前記記録媒体との間で機器認証を行う認証手段と、

機器認証が成功した場合にのみ、前記機器認証を経て得た固有鍵を用いて著作物を暗号化して記録媒体に転送し若しくは記録媒体から転送された著作物を復号する転送手段と

を備えることを特徴とするアクセス装置。

【請求項１０】　記録媒体とアクセス装置とが接続された状態で、両者間で機器認証ステップと著作物転送ステップとを実行して著作物の正当者への配布を実現するデジタル著作物保護方法であって、

機器認証ステップでは、記録媒体が所有する固有鍵をアクセス装置に秘密伝送し、アクセス装置が取得した固有鍵を用いて、機器認証を行い、

著作物転送ステップでは、機器認証が成功した場合にのみ、アクセス装置が取得した固有鍵を用いて著作物を暗号化して記録媒体に転送し若しくは記録媒体から転送された著作物を復号する

ことを特徴とするデジタル著作物保護方法。

【請求項１１】　記録媒体毎に異なる固有鍵を予め記憶している固有鍵記憶領域及び前記固有鍵を用いて暗号化される著作物を保持するための領域を有する記録媒体とアクセス装置とが接続された状態で、前記記録媒体と前記アクセス装置との間で機器認証と暗号化された著作物の転送とを行うデジタル著作物保護システムで用いられるデジタル著作物保護方法であって、

接続されたアクセス装置へ前記固有鍵を秘密伝送し、前記固有鍵を用いて前記アクセス装置との間で機器認証を行う第１認証ステップと、

記録媒体から秘密伝送された固有鍵を用いて、前記記録媒体との間で機器認証を行う第２認証ステップと、

機器認証が成功した場合にのみ、前記機器認証を経て得た固有鍵を用いて著作物を暗号化して記録媒体に転送し若しくは記録媒体から転送された著作物を復号する転送ステップとを

含むことを特徴とするデジタル著作物保護方法。

【請求項１２】　前記第１認証ステップは、あらかじめ第１鍵を有し、前記第１鍵を用いて、前記固有鍵に第１暗号を施して暗号化固有鍵を生成して伝送し、

前記第２認証ステップは、あらかじめ前記第１鍵を有し、前記第１鍵を用いて、前記伝送された暗号化固有鍵に、前記第１暗号の逆変換を行う第１復号を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器認証を行い、

前記転送ステップは、前記復号固有鍵を用いて著作物の転送を行う

ことを特徴とする請求項１１記載のデジタル著作物保護方法。

【請求項１３】　前記第１認証ステップは、第１鍵を基にして、公開鍵暗号方式の公開鍵決定アルゴリズムにより算出された公開鍵である第２鍵をあらかじめ有し、前記第２鍵を用いて、前記固有鍵に第１暗号を施して暗号化固有鍵を生成して伝送し、

前記第２認証ステップは、あらかじめ前記第１鍵を有し、前記第１鍵を用いて、前記伝送された暗号化固有鍵に、前記第１暗号の逆変換を行う第１復号を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器認証を行い、

前記転送ステップは、前記復号固有鍵を用いて著作物の転送を行う

ことを特徴とする請求項１１記載のデジタル著作物保護方法。

【請求項１４】　前記第１認証ステップは、あらかじめ第１鍵を有し、前記第１鍵を用いて、前記固有鍵に回復型署名処理を施して署名文を生成して伝送し、

前記第２認証ステップは、前記第１鍵に前記回復型署名処理の公開鍵決定アルゴリズムにより算出された公開鍵である第２鍵をあらかじめ有し、前記第２鍵を用いて、前記伝送された署名文に、前記回復型署名の検証処理を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器認証を行い、

前記転送ステップは、前記復号固有鍵を用いて著作物の転送を行う

ことを特徴とする請求項１１記載のデジタル著作物保護方法。

【請求項１５】　前記デジタル著作物保護システムは、さらに固有鍵に第１暗号を施して暗号化固有鍵に変換する固有鍵変換手段を備える暗号化固有鍵作成装置を有し、

前記第１認証ステップは、前記固有鍵を前記固有鍵変換手段へ出力して暗号化固有鍵に変換し、変換された暗号化固有鍵を前記アクセス装置へ伝送し、

前記第２認証ステップは、記録媒体から伝送された暗号化固有鍵に前記第１暗号の逆処理を行う第１復号を施して固有鍵を生成する

ことを特徴とする請求項１１記載のデジタル著作物保護方法。

【請求項１６】　前記第１認証ステップは、あらかじめ複数の第１鍵を有し、

前記複数の第１鍵のうち一つの第２鍵の選択を受け付け、前記第２鍵を用いて、前記固有鍵に第１暗号を施して暗号化固有鍵を生成して伝送し、

前記第２認証ステップは、あらかじめ複数の第１鍵を有し、前記複数の第１鍵から前記第２鍵の選択を受け付け、前記第２鍵を用いて、前記伝送された暗号化固有鍵に、前記第１暗号の逆変換を行う第１復号を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器認証を行い、

前記転送ステップは、前記復号固有鍵を用いて著作物の転送を行う

ことを特徴とする請求項１１記載のデジタル著作物保護方法。

【請求項１７】　デジタル著作物保護方法をコンピュータに実行させるためのプログラムを記録するコンピュータ読み取り可能な媒体であって、

請求項１０～１６記載の何れかのデジタル著作物保護方法をコンピュータに実行させるためのプログラムを含むことを特徴とする記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、デジタル化された文書、音声、画像、プログラムなどのデジタル著作物をネットワークで配信し、これを記憶媒体に記録し、携帯プレーヤで再生するシステムに関し、特に、不正にこれらの記録や再生が行われることを防ぐシステムに関する。

【０００２】

【従来の技術】

近年、デジタル化された文書、音声、画像、プログラムなどのデジタル著作物がインターネットなどのネットワークを経由して流通し、利用者は、様々なデジタル著作物を簡単にネットワークを経由して取り出し、他の記録媒体に記録し、再生することができるようになってきている。

【０００３】

【発明が解決しようとする課題】

しかしながら、このように簡単にデジタル著作物を複製できるという利点はあるものの、著作者の著作権が侵害されやすいという問題点がある。

本発明は、外部から取り出したデジタル著作物を不正に記録媒体へ書き込むことと、記録媒体に記録されたデジタル著作物を不正に再生することを防止するデジタル著作物保護システムを提供することを目的とする。

【０００４】

【課題を解決するための手段】

上記の目的を達成するために、本発明は、記録媒体とアクセス装置とが接続された状態で、両者間で機器認証フェーズと著作物転送フェーズとを実行して著作物の正当者への配布を実現するデジタル著作物保護システムであって、機器認証フェーズでは、記録媒体が所有する固有鍵をアクセス装置に秘密伝送し、アクセス装置が取得した固有鍵を用いて、機器認証を行い、著作物転送フェーズでは、機器認証が成功した場合にのみ、アクセス装置が取得した固有鍵を用いて著作物を暗号化して記録媒体に転送し若しくは記録媒体から転送された著作物を復号することを特徴とする。

【０００５】

ここで、記録媒体とアクセス装置とが接続された状態で、前記記録媒体と前記アクセス装置との間で機器認証と暗号化された著作物の転送とを行うデジタル著作物保護システムであって、前記記録媒体は、記録媒体毎に異なる固有鍵を予め記憶している固有鍵記憶領域と、接続されたアクセス装置へ前記固有鍵を秘密伝送し、前記固有鍵を用いて前記アクセス装置との間で機器認証を行う第１認証手段と、前記固有鍵を用いて暗号化される著作物を保持するための領域とを備え、前記アクセス装置は、記録媒体から秘密伝送された固有鍵を用いて、前記記録媒体との間で機器認証を行う第２認証手段と、機器認証が成功した場合にのみ、前記機器認証を経て得た固有鍵を用いて著作物を暗号化して記録媒体に転送し若しくは記録媒体から転送された著作物を復号する転送手段とを備えるように構成してもよい。

【０００６】

ここで、前記第１認証手段は、あらかじめ第１鍵を有し、前記第１鍵を用いて、前記固有鍵に第１暗号を施して暗号化固有鍵を生成して伝送し、前記第２認証手段は、あらかじめ前記第１鍵を有し、前記第１鍵を用いて、前記伝送された暗

号化固有鍵に、前記第１暗号の逆変換を行う第１復号を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器認証を行い、前記転送手段は、前記復号固有鍵を用いて著作物の転送を行うように構成してもよい。

【０００７】

ここで、前記第１認証手段は、第１鍵を基にして、公開鍵暗号方式の公開鍵決定アルゴリズムにより算出された公開鍵である第２鍵をあらかじめ有し、前記第２鍵を用いて、前記固有鍵に第１暗号を施して暗号化固有鍵を生成して伝送し、前記第２認証手段は、あらかじめ前記第１鍵を有し、前記第１鍵を用いて、前記伝送された暗号化固有鍵に、前記第１暗号の逆変換を行う第１復号を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器認証を行い、前記転送手段は、前記復号固有鍵を用いて著作物の転送を行うように構成してもよい。

【０００８】

ここで、前記第１認証手段は、あらかじめ第１鍵を有し、前記第１鍵を用いて、前記固有鍵に回復型署名処理を施して署名文を生成して伝送し、前記第２認証手段は、前記第１鍵に前記回復型署名処理の公開鍵決定アルゴリズムにより算出された公開鍵である第２鍵をあらかじめ有し、前記第２鍵を用いて、前記伝送された署名文に、前記回復型署名の検証処理を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器認証を行い、前記転送手段は、前記復号固有鍵を用いて著作物の転送を行うように構成してもよい。

【０００９】

ここで、前記デジタル著作物保護システムは、さらに固有鍵に第１暗号を施して暗号化固有鍵に変換する固有鍵変換手段を備える暗号化固有鍵作成装置を有し、前記第１認証手段は、前記固有鍵を前記固有鍵変換手段へ出力して暗号化固有鍵に変換し、変換された暗号化固有鍵を前記アクセス装置へ伝送し、前記第２認証手段は、記録媒体から伝送された暗号化固有鍵に前記第１暗号の逆処理を行う第１復号を施して固有鍵を生成するように構成してもよい。

【００１０】

ここで、前記第１認証手段は、あらかじめ複数の第１鍵を有し、前記複数の第

１鍵のうち一つの第２鍵の選択を受け付け、前記第２鍵を用いて、前記固有鍵に第１暗号を施して暗号化固有鍵を生成して伝送し、前記第２認証手段は、あらかじめ複数の第１鍵を有し、前記複数の第１鍵から前記第２鍵の選択を受け付け、前記第２鍵を用いて、前記伝送された暗号化固有鍵に、前記第１暗号の逆変換を行う第１復号を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器認証を行い、前記転送手段は、前記復号固有鍵を用いて著作物の転送を行うように構成してもよい。

【００１１】

また、本発明は、アクセス装置と接続された状態で、前記アクセス装置との間で機器認証と暗号化された著作物の転送とを行う記録媒体であって、記録媒体毎に異なる固有鍵を記憶している固有鍵記憶領域と、前記固有鍵を用いて暗号化される著作物を保持するための領域と、アクセス装置が接続されたとき、記録媒体から当該アクセス装置へ固有鍵を秘密伝送する手順を経て、当該アクセス装置との間で機器認証を行う認証手段と、機器認証が成功した場合にのみ、前記固有鍵を用いて暗号化された著作物を受け取り前記領域に書き込み若しくは前記領域に記憶されている暗号化された著作物を読み出して前記アクセス装置へ出力する転送手段とを備えることを特徴とする。

【００１２】

また、本発明は、固有鍵を有する記録媒体と接続され、前記記録媒体との間で機器認証と暗号化された著作物の転送とを行うアクセス装置であって、記録媒体から固有鍵を秘密伝送される手順を経て、前記記録媒体との間で機器認証を行う認証手段と、機器認証が成功した場合にのみ、前記機器認証を経て得た固有鍵を用いて著作物を暗号化して記録媒体に転送し若しくは記録媒体から転送された著作物を復号する転送手段とを備えることを特徴とする。

【００１３】

【発明の実施の形態】

本発明に係る一つの実施の形態としてのデジタル著作物保護システム１００について説明する。

１．　デジタル著作物保護システム１００の構成

デジタル著作物保護システム１００は、図１のブロック図に示すように、メモリカード２００、メモリカードライタ３００、メモリカードリーダ４００から構成される。

【００１４】

メモリカード２００は、図２に示すように、メモリカード挿入口３０１から挿入され、メモリカードライタ３００に装着される。また、メモリカードライタ３００は、メモリカードライタ挿入口５０１から挿入され、パーソナルコンピュータ５００に装着される。メモリカードライタ３００は、パーソナルコンピュータ５００を介在して通信回線１０により外部と接続されている。

【００１５】

パーソナルコンピュータ５００は、ディスプレイ５０３、キーボード５０４、スピーカ５０２、図示していないプロセッサ、ＲＡＭ、ＲＯＭ、ハードディスク装置を備えている。

メモリカード２００は、メモリカードリーダ４００に装着される。メモリカード２００は、図３に示すように、メモリカード挿入口４０３から挿入されて、メモリカードリーダ４００の一つの実施例としてのヘッドホンステレオ４０１に装着される。ヘッドホンステレオ４０１は、上面に操作ボタン４０４ａ、４０４ｂ、４０４ｃ、４０４ｄが配置され、側面にメモリカード挿入口４０３を有し、別の側面にヘッドホン４０２が接続されている。

１．１　メモリカード２００の構成

メモリカード２００は、図４に示すように、マスタ鍵記憶部２１０、メディア固有鍵記憶部２２０、変換部２３０、メディア固有鍵情報記憶部２４０、装置鍵記憶部２２１、逆変換部２２２、装置鍵情報記憶部２２３、相互認証部２５０、暗号化著作物記憶部２６０、通信部２７０、制御部２８０から構成される。

【００１６】

メモリカード２００がメモリカードライタ３００に装着されると、通信部２７０は、メモリカードライタ３００の後述する通信部３４０と接続される。

メモリカード２００がメモリカードリーダ４００に装着されると、通信部２７０は、メモリカードリーダ４００の後述する通信部４４０と接続される。

１．１．１　マスタ鍵記憶部２１０

マスタ鍵記憶部２１０は、あらかじめ一つのマスタ鍵Mk を記憶している。マスタ鍵Mk は、５６ビットのビット列からなる。マスタ鍵は、デジタル著作物運用システム毎に異なる。さらに、特定のデジタル著作物運用システム用メモリカードを製造するすべてのメーカにより製造されたすべてのメモリカードのマスタ鍵記憶部には、同じマスタ鍵が記憶されている。

【００１７】

ここで、デジタル著作物運用システムとは、例えば、Ａ社、Ｂ社、Ｃ社の３者が共同で運営し、音楽を配信する音楽配信システムであり、また、Ｘ社、Ｙ社、Ｚ社が共同で運営する映画レンタルシステムである。

１．１．２　メディア固有鍵記憶部２２０

メディア固有鍵記憶部２２０は、あらかじめ一つの固有鍵Ｋｉ を記憶している。固有鍵Ｋｉ は、５６ビットのビット列からなる。固有鍵は、メモリカード毎に異なる。固有鍵は、メモリカード毎に異なるメモリカードの製造番号と、その都度生成される乱数とに、所定の演算を施して、例えば加算を施して算出される。

１．１．３　変換部２３０

変換部２３０は、メディア固有鍵記憶部２２０に記憶されている固有鍵Ｋｉ を読み出し、マスタ鍵記憶部２１０に記憶されているマスタ鍵Mk を読み出す。

【００１８】

変換部２３０は、ＤＥＳ（データ暗号化規格、Ｄａｔａ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）により規格されている暗号アルゴリズムＥ1 をあらかじめ記憶している。

ここで、ＤＥＳにより規格されている暗号アルゴリズムＥ1 は、暗号鍵は５６ビットであり、平文及び暗号文の長さは６４ビットである。なお、この実施の形

態において、暗号アルゴリズム及び復号アルゴリズムは、特に断らない限り、ＤＥＳにより規格されているアルゴリズムであり、暗号鍵及び復号鍵は５６ビットであり、平文及び暗号文の長さは６４ビットである。

【００１９】

変換部２３０は、読み出した固有鍵Ｋｉ に暗号アルゴリズムＥ1 を施して暗号化固有鍵Ｊｉ を生成する。このとき、前記読み出したマスタ鍵Ｍｋ を暗号アルゴリズムＥ1 の鍵とする。生成された暗号化固有鍵Ｊｉ は式１に示すように表現できる。

（式１）　Ｊｉ ＝Ｅ1 （Ｍｋ 、Ｋｉ ）

なお、この明細書において、鍵Ｋを用いて、平文Ｍに対して、暗号アルゴリズムＥを施し、暗号文Ｃを生成するとき、式２に示すように表現することとする。

（式２）　Ｃ＝Ｅ（Ｋ、Ｍ）

また、鍵Ｋを用いて、前記生成された暗号文Ｃに対して、復号アルゴリズムＤを施して、前記平文Ｍを生成するとき、式３に示すように表現することとする。

（式３）　Ｍ＝Ｄ（Ｋ、Ｃ）

このように、鍵Ｋを用いて、平文Ｍに対して、暗号アルゴリズムＥを施し暗号文Ｃを生成し、生成された暗号文Ｃに対して、復号アルゴリズムＤを施して、前記平文Ｍと同一の平文が生成されるとき、暗号アルゴリズムＥと復号アルゴリズムＤとの関係を式４に示すように表現することとする。

（式４）　Ｅ＝Ｄ-1

変換部２３０は、生成した暗号化固有鍵Ｊｉ をメディア固有鍵情報記憶部２４０へ出力する。

１．１．４　メディア固有鍵情報記憶部２４０

メディア固有鍵情報記憶部２４０は、変換部２３０から、暗号化固有鍵Ｊｉ を受け取り、受け取った暗号化固有鍵Ｊｉ を記憶する。

１．１．５　相互認証部２５０

相互認証部２５０は、乱数発生部２５１、暗号部２５２、復号部２５３、相互

認証制御部２５４から構成される。

（１）乱数発生部２５１

乱数発生部２５１は、乱数Ｒ2 を生成する。乱数Ｒ2 は、６４ビットのビット列からなる。乱数発生部２５１は、生成した乱数Ｒ2 を通信部２７０と相互認証制御部２５４とへ出力する。

（２）暗号部２５２

暗号部２５２は、通信部２７０から乱数Ｒ1 を受け取る。

【００２０】

暗号部２５２は、メディア固有鍵記憶部２２０から固有鍵Ｋｉ を読み出す。

暗号部２５２は、ＤＥＳにより規格されている暗号アルゴリズムＥ2 をあらかじめ記憶している。

暗号部２５２は、受け取った乱数Ｒ1 に暗号アルゴリズムＥ2 を施して暗号化乱数Ｓ1 を生成する。このとき、前記読み出した固有鍵Ｋｉ を暗号アルゴリズムＥ2 の鍵とする。生成された暗号化乱数Ｓ1 は式５に示すように表現できる。

（式５）　Ｓ1 ＝Ｅ2 （Ｋｉ 、Ｒ1 ）

暗号部２５２は、生成した暗号化乱数Ｓ1 を通信部２７０へ出力する。

（３）復号部２５３

復号部２５３は、通信部２７０から暗号化乱数Ｓ2 を受け取り、装置鍵記憶部２２１から装置鍵Ａ’ｊ を読み出す。

【００２１】

復号部２５３は、ＤＥＳにより規格されている復号アルゴリズムＤ2 をあらかじめ記憶している。

復号部２５３は、受け取った暗号化乱数Ｓ2 に復号アルゴリズムＤ2 を施して乱数Ｒ’２ を生成する。このとき、前記読み出した装置鍵Ａ’ｊ を復号アルゴリズムＤ2 の鍵とする。生成された乱数Ｒ’２ は式６に示すように表現できる。

（式６）　Ｒ’２ ＝Ｄ2 （Ａ’ｊ 、Ｓ2 ）

＝D2（A’j、E2（Aj、R2））

復号部２５３は、生成した乱数R’２を相互認証制御部２５４へ出力する。

（４）相互認証制御部２５４

相互認証制御部２５４は、復号部２５３から乱数R’２を受け取る。また、相互認証制御部２５４は、乱数発生部２５１から乱数R2を受け取る。

【００２２】

相互認証制御部２５４は、復号部２５３から受け取った乱数R’２と、乱数発生部２５１から受け取った乱数R2とを比較し、乱数R’２と乱数R2とが一致すれば、メモリカード２００が装着されたメモリカードライタ３００又はメモリカードリーダ４００が正しい装置であると認証し、乱数R’２と乱数R2とが一致していなければ、メモリカード２００が装着されたメモリカードライタ３００又はメモリカードリーダ４００が不正な装置であるとみなす。

【００２３】

相互認証制御部２５４は、メモリカードライタ３００又はメモリカードリーダ４００が正しい装置であるか、不正な装置であるかを示す認証信号を制御部２８０へ出力する。

１．１．６　暗号化著作物記憶部２６０

暗号化著作物記憶部２６０は、記憶媒体として半導体メモリを有する。

【００２４】

暗号化著作物記憶部２６０は、通信部２７０から暗号化部分著作物Fi（i＝1、2、3、・・・）を受け取り、受け取った暗号化部分著作物Fi（i＝1、2、3、・・・）を記憶する。

１．１．７　通信部２７０

通信部２７０は、メディア固有鍵情報記憶部２４０から暗号化固有鍵Jiを読み出し、読み出した暗号化固有鍵Jiをメモリカードライタ３００の通信部３４０又はメモリカードリーダ４００の通信部４４０へ出力する。

【００２５】

通信部２７０は、メモリカードライタ３００の通信部３４０から又はメモリカードリーダ４００の通信部４４０から乱数Ｒ1 を受け取り、受け取った乱数Ｒ1 を相互認証部２５０の暗号部２５２へ出力する。

通信部２７０は、暗号部２５２から暗号化乱数Ｓ1 を受け取り、受け取った暗号化乱数Ｓ1 をメモリカードライタ３００の通信部３４０又はメモリカードリーダ４００の通信部４４０へ出力する。

【００２６】

通信部２７０は、メモリカードライタ３００の通信部３４０又はメモリカードリーダ４００の通信部４４０から、暗号化装置鍵Ｂｊ を受け取り、受け取った暗号化装置鍵Ｂｊ を装置鍵情報記憶部２２３へ出力する。

通信部２７０は、乱数発生部２５１から乱数Ｒ2 を受け取り、受け取った乱数Ｒ2 をメモリカードライタ３００の通信部３４０又はメモリカードリーダ４００の通信部４４０へ出力する。

【００２７】

通信部２７０は、メモリカードライタ３００の通信部３４０又はメモリカードリーダ４００の通信部４４０から暗号化乱数Ｓ2 を受け取り、受け取った暗号化乱数Ｓ2 を相互認証部２５０の復号部２５３へ出力する。

通信部２７０は、制御部２８０から通信中止信号を受け取ると、メモリカードライタ３００の通信部３４０又はメモリカードリーダ４００の通信部４４０との通信を中止する。

【００２８】

通信部２７０は、メモリカードライタ３００の通信部３４０から暗号化部分著作物Ｆｉ （ｉ＝１、２、３、・・・）を受け取り、受け取った暗号化部分著作物Ｆｉ （ｉ＝１、２、３、・・・）を暗号化著作物記憶部２６０へ出力する。

通信部２７０は、暗号化著作物記憶部２６０から暗号化著作物を読み出し、読み出した暗号化著作物をメモリカードリーダ４００の通信部４４０へ出力する。

１．１．８　装置鍵情報記憶部２２３

装置鍵情報記憶部２２３は、通信部２７０から暗号化装置鍵Ｂｊ を受け取り、

受け取った暗号化装置鍵Ｂｊ を記憶する。

１．１．９　逆変換部２２２

逆変換部２２２は、装置鍵情報記憶部２２３から暗号化装置鍵Ｂｊ を読み出し、マスタ鍵記憶部２１０に記憶されているマスタ鍵Mk を読み出す。

【００２９】

逆変換部２２２は、ＤＥＳにより規格されている復号アルゴリズムD3 をあらかじめ記憶している。

逆変換部２２２は、読み出した暗号化装置鍵Ｂｊ に復号アルゴリズムD3 を施して装置鍵Ａ’ｊ を生成する。このとき、前記読み出したマスタ鍵Mk を復号アルゴリズムD3 の鍵とする。生成された装置鍵Ａ’ｊ は式７に示すように表現できる。

（式７）　Ａ’ｊ＝D3（Mk、Ｂｊ）

＝D3（Mk、E3（Mk、Ａｊ））

逆変換部２２２は、生成した装置鍵Ａ’ｊ を装置鍵記憶部２２１へ出力する。

１．１．１０　装置鍵記憶部２２１

装置鍵記憶部２２１は、逆変換部２２２から出力された装置鍵Ａ’ｊ を記憶する。

１．１．１１　制御部２８０

制御部２８０は、相互認証制御部２５４からメモリカード２００が装着されたメモリカードライタ３００又はメモリカードリーダ４００が正しい装置であるか、不正な装置であるかを示す認証信号を受け取る。

【００３０】

制御部２８０は、受け取った認証信号が不正な装置であることを示す場合には、メモリカードライタ３００又はメモリカードリーダ４００との通信を中止する通信中止信号を通信部２７０へ出力する。

１．２　メモリカードライタ３００の構成

メモリカードライタ３００は、図５に示すように、装置鍵記憶部３１０、変換部３１１、装置鍵情報記憶部３１２、マスタ鍵記憶部３１３、メディア固有鍵情報記憶部３２０、逆変換部３２１、メディア固有鍵記憶部３２３、相互認証部３３０、通信部３４０、制御部３５０、暗号部３６０、著作物記憶部３７０、著作物取得部３８０から構成される。

【００３１】

著作物取得部３８０は、通信回線１０を経由して外部と接続されている。

１．２．１　装置鍵記憶部３１０

装置鍵記憶部３１０は、あらかじめ一つの装置鍵Ａｊ を記憶している。装置鍵Ａｊ は、５６ビットのビット列からなる。装置鍵は、メモリカードライタ毎に異なる。装置鍵は、メモリカードライタ毎に異なるメモリカードライタの製造番号と、その都度生成される乱数とに、所定の演算を施して、例えば加算を施して算出される。

１．２．２　変換部３１１

変換部３１１は、装置鍵記憶部３１０に記憶されている装置鍵Ａｊ を読み出し、マスタ鍵記憶部３１３に記憶されているマスタ鍵Mk を読み出す。

【００３２】

変換部３１１は、ＤＥＳにより規格されている暗号アルゴリズムＥ3 をあらかじめ記憶している。

メモリカード２００の逆変換部２２２に記憶されている復号アルゴリズムＤ3 と暗号アルゴリズムＥ3 との間には、式８に示す関係がある。

（式８）　$E3 = D3^{-1}$

変換部３１１は、読み出した装置鍵Ａｊ に暗号アルゴリズムＥ3 を施して暗号化装置鍵Ｂｊ を生成する。このとき、前記読み出したマスタ鍵Mk を暗号アルゴリズムＥ3 の鍵とする。生成された暗号化装置鍵Ｂｊ は式９に示すように表現できる。

（式９）　Ｂｊ ＝Ｅ3 （Mk 、Ａｊ ）

変換部３１１は、生成した暗号化装置鍵Ｂｊ を装置鍵情報記憶部３１２へ出力する。

１．２．３　装置鍵情報記憶部３１２

装置鍵情報記憶部３１２は、変換部３１１から暗号化装置鍵Ｂｊ を受け取り、受け取った暗号化装置鍵Ｂｊ を記憶する。

１．２．４　マスタ鍵記憶部３１３

マスタ鍵記憶部３１３は、あらかじめ一つのマスタ鍵Mk を記憶している。マスタ鍵Mk は、メモリカード２００のマスタ鍵記憶部２１０が記憶しているマスタ鍵と同じである。

１．２．５　メディア固有鍵情報記憶部３２０

メディア固有鍵情報記憶部３２０は、通信部３４０から暗号化固有鍵Ｊｉ を受け取り、受け取った暗号化固有鍵Ｊｉ を記憶する。

１．２．６　逆変換部３２１

逆変換部３２１は、メディア固有鍵情報記憶部３２０に記憶されている暗号化固有鍵Ｊｉ を読み出し、マスタ鍵記憶部３１３に記憶されているマスタ鍵Mk を読み出す。

【００３３】

逆変換部３２１は、ＤＥＳにより規格されている復号アルゴリズムD1 をあらかじめ記憶している。

メモリカード２００の変換部２３０に記憶されている暗号アルゴリズムＥ1 と復号アルゴリズムD1 との間には、式１０に示す関係がある。

（式１０）　$E1 = D1^{-1}$

逆変換部３２１は、読み出した暗号化固有鍵Ｊｉ に復号アルゴリズムD1 を施して固有鍵Ｋ’ｉ を生成する。このとき、前記読み出したマスタ鍵Mk を復号アルゴリズムD1 の鍵とする。生成された固有鍵Ｋ’ｉ は、式１１に示すように表

現できる。

（式１１）　K’ｉ＝D1（Mk、Ｊｉ）

＝D1（Mk、E1（Mk、Ki））

逆変換部３２１は、生成した固有鍵K’ｉをメディア固有鍵記憶部３２３へ出力する。

１．２．７　メディア固有鍵記憶部３２３

メディア固有鍵記憶部３２３は、逆変換部３２１から固有鍵K’ｉを受け取り、受け取った固有鍵K’ｉを記憶する。

１．２．８　相互認証部３３０

相互認証部３３０は、乱数発生部３３１、暗号部３３２、復号部３３３、相互認証制御部３３４から構成される。

（１）乱数発生部３３１

乱数発生部３３１は、乱数R1を生成する。乱数R1は、６４ビットのビット列からなる。乱数発生部３３１は、生成した乱数R1を通信部３４０へ出力する。また、乱数発生部３３１は、生成した乱数R1を相互認証制御部３３４へ出力する。

（２）暗号部３３２

暗号部３３２は、通信部３４０から乱数R2を受け取り、装置鍵記憶部３１０から装置鍵Ａｊを読み出す。

【００３４】

暗号部３３２は、ＤＥＳにより規格されている暗号アルゴリズムE2をあらかじめ記憶している。

暗号部３３２は、受け取った乱数R2に暗号アルゴリズムE2を施して暗号化乱数S2を生成する。このとき、前記読み出した装置鍵Ａｊを暗号アルゴリズムE2の鍵とする。生成された暗号化乱数S2は式１２に示すように表現できる。

（式１２）　S2 ＝E2 （Aj 、R2 ）

暗号部３３２は、生成した暗号化乱数Ｓ2 を通信部３４０へ出力する。

（３）復号部３３３

復号部３３３は、通信部３４０から暗号化乱数Ｓ1 を受け取る。

【００３５】

復号部３３３は、メディア固有鍵記憶部３２３から固有鍵K’ｉ を読み出す。

復号部３３３は、ＤＥＳにより規格されている復号アルゴリズムD2 をあらかじめ記憶している。

メモリカード２００の相互認証部３３０の暗号部２５２に記憶されている暗号アルゴリズムE2 と復号アルゴリズムD2 との間には、式１３に示す関係がある。

（式１３）　$E2 = D2^{-1}$

復号部３３３は、受け取った暗号化乱数Ｓ1 に復号アルゴリズムD2 を施して乱数R’１ を生成する。このとき、前記読み出した固有鍵K’ｉ を復号アルゴリズムD2 の鍵とする。生成された乱数R’１ は式１４に示すように表現できる。

（式１４）　R’１ ＝D2 （K’ｉ 、Ｓ1 ）

＝D2 （K’ｉ 、E2 （Ki 、R1 ））

復号部３３３は、生成された乱数R’１ を相互認証制御部３３４へ出力する。

（４）相互認証制御部３３４

相互認証制御部３３４は、復号部３３３から乱数R’１ を受け取る。また、相互認証制御部３３４は、乱数発生部３３１から乱数R1 を受け取る。

【００３６】

相互認証制御部３３４は、復号部３３３から受け取った乱数R’１ と、乱数発生部３３１から受け取った乱数R1 とを比較し、乱数R’１ と乱数R1 とが一致すれば、メモリカードライタ３００に装着されたメモリカード２００が正しい装置であると認証し、乱数R’１ と乱数R1 とが一致していなければ、メモリカードライタ３００に装着されたメモリカード２００が不正な装置であるとみなす。

【００３７】

相互認証制御部３３４は、メモリカードライタ３００に装着されたメモリカード２００が正しい装置であるか、不正な装置であるかを示す認証信号を制御部３５０へ出力する。

１．２．９　通信部３４０

通信部３４０は、メモリカード２００の通信部２７０から暗号化固有鍵Ｊｉ を受け取り、受け取った暗号化固有鍵Ｊｉ をメディア固有鍵情報記憶部３２０へ出力する。

【００３８】

通信部３４０は、乱数発生部３３１から乱数Ｒ1 を受け取り、受け取った乱数Ｒ1 を、メモリカード２００の通信部２７０へ出力する。

通信部３４０は、メモリカード２００の通信部２７０から暗号化乱数Ｓ1 を受け取り、受け取った暗号化乱数Ｓ1 を相互認証部３３０の復号部３３３へ出力する。

【００３９】

通信部３４０は、装置鍵情報記憶部３１２から暗号化装置鍵Ｂｊ を読み出し、読み出した暗号化装置鍵Ｂｊ をメモリカード２００の通信部２７０へ出力する。

通信部３４０は、メモリカード２００の通信部２７０から乱数Ｒ2 を受け取り、受け取った乱数Ｒ2 を相互認証部３３０の暗号部３３２へ出力する。

通信部３４０は、暗号部３３２から暗号化乱数Ｓ2 を受け取り、受け取った暗号化乱数Ｓ2 をメモリカード２００の通信部２７０へ出力する。

【００４０】

通信部３４０は、制御部３５０から通信中止信号を受け取ると、メモリカード２００の通信部２７０との通信を中止する。

通信部３４０は、暗号部３６０から暗号化部分著作物Ｆｉ （ｉ＝１、２、３、・・・）を受け取り、受け取った暗号化部分著作物Ｆｉ （ｉ＝１、２、３、・・・）をメモリカード２００の通信部２７０へ出力する。

１．２．１０　制御部３５０

制御部３５０は、相互認証制御部３３４からメモリカードライタ３００に装着されたメモリカード２００が正しい装置であるか、不正な装置であるかを示す認証信号を受け取る。

【００４１】

制御部３５０は、受け取った認証信号が不正な装置であることを示す場合には、メモリカード２００との通信を中止する通信中止信号を通信部３４０へ出力する。

制御部３５０は、受け取った認証信号が正しい装置であることを示す場合には、著作物取得部３８０に対して、外部からの著作物取得を指示する著作物取得信号を出力する。

１．２．１１　著作物取得部３８０

著作物取得部３８０は、制御部３５０から著作物取得信号を受け取る。

【００４２】

著作物取得部３８０は、制御部３５０から著作物取得信号を受け取ると、通信回線１０を経由して、外部から音楽の著作物を取得し、取得した著作物を著作物記憶部３７０へ出力する。

１．２．１２　著作物記憶部３７０

著作物記憶部３７０は、著作物取得部３８０から著作物を受け取り、受け取った著作物を記憶する。

１．２．１３　暗号部３６０

暗号部３６０は、著作物記憶部３７０から著作物を読み出し、メディア固有鍵記憶部３２３から固有鍵K’ｉを読み出す。

【００４３】

暗号部３６０は、ＤＥＳにより規格されている暗号アルゴリズムE2 をあらかじめ記憶している。

暗号部３６０は、読み出した著作物を複数の６４ビットのビット列からなる部

分著作物Ｃｉ（ｉ＝１、２、３、・・・）に分割し、各部分著作物Ｃｉ（ｉ＝１、２、３、・・・）に暗号アルゴリズムＥ2 を施して複数の暗号化部分著作物Ｆｉ（ｉ＝１、２、３、・・・）を生成する。このとき、前記読み出した固有鍵Ｋ’ｉを暗号アルゴリズムＥ2 の鍵とする。生成された暗号化部分著作物Ｆｉ（ｉ＝１、２、３、・・・）は式１５に示すように表現できる。

（式１５）　Ｆｉ＝Ｅ2（Ｋ’ｉ、Ｃｉ）　（ｉ＝１、２、３、・・・）

暗号部３６０は、生成した暗号化部分著作物Ｆｉ（ｉ＝１、２、３、・・・）を通信部３４０へ出力する。

１．３　メモリカードリーダ４００の構成

メモリカードライタ３００は、図６に示すように、装置鍵記憶部４１０、変換部４１１、装置鍵情報記憶部４１２、マスタ鍵記憶部４１３、メディア固有鍵情報記憶部４２０、逆変換部４２１、メディア固有鍵記憶部４２３、相互認証部４３０、通信部４４０、制御部４５０、復号部４６０、著作物記憶部４７０、再生部４８０、操作部４９０から構成される。

【００４４】

装置鍵記憶部４１０、変換部４１１、装置鍵情報記憶部４１２、マスタ鍵記憶部４１３、メディア固有鍵情報記憶部４２０、逆変換部４２１、メディア固有鍵記憶部４２３、相互認証部４３０、通信部４４０、制御部４５０については、それぞれメモリカードリーダ４００の装置鍵記憶部３１０、変換部３１１、装置鍵情報記憶部３１２、マスタ鍵記憶部３１３、メディア固有鍵情報記憶部３２０、逆変換部３２１、メディア固有鍵記憶部３２３、相互認証部３３０、通信部３４０、制御部３５０と同等であるので、同等部分の説明は省略し、異なる機能、作用を有する点を中心として説明する。

１．３．１　制御部４５０

制御部４５０は、受け取った認証信号が正しい装置であることを示す場合には、復号部４６０に対して、通信部４４０から出力される暗号化著作物の復号を指示する復号指示を出力する。

１．３．２　復号部４６０

復号部４６０は、制御部４５０から復号指示を受け取る。

【００４５】

復号部４６０は、制御部４５０から復号指示を受け取ると、通信部４４０から暗号化著作物を受け取り、メディア固有鍵記憶部４２３から固有鍵K’ｉを読み出す。

復号部４６０は、ＤＥＳにより規格されている復号アルゴリズムD2 をあらかじめ記憶している。

【００４６】

復号部４６０は、受け取った暗号化著作物を複数の６４ビットのビット列からなる部分暗号化著作物Ｇｉ（ｉ＝１、２、３、・・・）に分割し、各部分暗号化著作物Ｇｉ（ｉ＝１、２、３、・・・）に復号アルゴリズムD2 を施して複数の部分著作物Ｈｉ（ｉ＝１、２、３、・・・）を生成する。このとき、前記読み出した固有鍵K’ｉを復号アルゴリズムD2 の鍵とする。生成された部分著作物Ｈｉ（ｉ＝１、２、３、・・・）は式１６に示すように表現できる。

（式１６）　Ｈｉ＝D2（K’ｉ、Ｇｉ）　（ｉ＝１、２、３、・・・）

復号部４６０は、生成した部分著作物Ｈｉ（ｉ＝１、２、３、・・・）を著作物記憶部４７０へ出力する。

１．３．３　著作物記憶部４７０

著作物記憶部４７０は、復号部４６０から部分著作物Ｈｉ（ｉ＝１、２、３、・・・）を受け取り、受け取った部分著作物Ｈｉ（ｉ＝１、２、３、・・・）を記憶する。

１．３．４　操作部４９０

操作部４９０は、各種のユーザの指示を受け付ける複数の操作ボタンを有している。

【００４７】

各種のユーザの指示に対応する操作ボタンが、ユーザにより操作されると、操作された操作ボタンに対応する指示を再生部４８０に出力する。

１．３．５　再生部４８０

再生部４８０は、操作部４９０から指示を受け取る。

【００４８】

再生部４８０は、受け取った指示に基づいて、著作物記憶部４７０に記憶されている音楽の著作物を読み出し、読み出した著作物を再生する。

２．　デジタル著作物保護システム１００の動作

デジタル著作物保護システム１００の動作について説明する。

２．１　メモリカード２００がメモリカードライタ３００に装着された場合の概要動作

メモリカード２００が、メモリカードライタ３００に装着された場合の概要動作について、図７に示すフローチャートを用いて説明する。

【００４９】

メモリカード２００が、メモリカードライタ３００に装着されると、メモリカードライタ３００がメモリカード２００を認証し（ステップＳ１１０）、メモリカードライタ３００が、メモリカード２００は不正な装置であると認識した場合には（ステップＳ１１１）、メモリカードライタ３００とメモリカード２００との間で通信を行わず、処理を終了する。

【００５０】

メモリカードライタ３００が、メモリカード２００は正しい装置であると認識した場合には（ステップＳ１１１）、メモリカード２００がメモリカードライタ３００を認証し（ステップＳ１１２）、メモリカード２００が、メモリカードライタ３００は不正な装置であると認識した場合には（ステップＳ１１３）、メモリカードライタ３００とメモリカード２００との間で通信を行わず、処理を終了する。

【００５１】

メモリカード２００が、メモリカードライタ３００は正しい装置であると認識した場合には（ステップＳ１１３）、メモリカードライタ３００は、外部から著作物を取得し、取得した著作物を暗号化し、メモリカード２００へ出力し（ステップＳ１１４）、メモリカード２００は、暗号化された著作物を記憶する（ステップＳ１１５）。

２．２　メモリカード２００がメモリカードリーダ４００に装着された場合の概要動作

メモリカード２００が、メモリカードリーダ４００に装着された場合の概要動作について、図８に示すフローチャートを用いて説明する。

【００５２】

メモリカード２００が、メモリカードリーダ４００に装着されると、メモリカードリーダ４００がメモリカード２００を認証し（ステップＳ１２０）、メモリカードリーダ４００が、メモリカード２００は不正な装置であると認識した場合には（ステップＳ１２１）、メモリカードリーダ４００とメモリカード２００との間で通信を行わず、処理を終了する。

【００５３】

メモリカードリーダ４００が、メモリカード２００は正しい装置であると認識した場合には（ステップＳ１２１）、メモリカード２００がメモリカードリーダ４００を認証し（ステップＳ１２２）、メモリカード２００が、メモリカードリーダ４００は不正な装置であると認識した場合には（ステップＳ１２３）、メモリカードリーダ４００とメモリカード２００との間で通信を行わず、処理を終了する。

【００５４】

メモリカード２００が、メモリカードリーダ４００は正しい装置であると認識した場合には（ステップＳ１２３）、メモリカード２００は、暗号化された著作物をメモリカードリーダ４００へ出力し（ステップＳ１２４）、メモリカードリ

ーダ４００は、メモリカード２００から出力された暗号された著作物を復号し（ステップＳ１２５）、メモリカードリーダ４００は復号された著作物を再生する（ステップＳ１２６）。

２．３　メモリカード２００がメモリカードライタ３００に装着された場合の詳細の認証動作

メモリカード２００が、メモリカードライタ３００に装着された場合の詳細の認証動作について、図９及び図１０を用いて説明する。

【００５５】

変換部２３０は、マスタ鍵Mk を暗号アルゴリズムE1 の鍵として、固有鍵Ｋｉに暗号アルゴリズムE1 を施して暗号化固有鍵E1 （Mk 、Ｋｉ）を生成し（ステップＳ１３０）、通信部２７０は、暗号化固有鍵E1 （Mk 、Ｋｉ）を通信部３４０を経由して逆変換部３２１へ出力し（ステップＳ１３１）、逆変換部３２１は、マスタ鍵Mk を復号アルゴリズムD1 の鍵として、暗号化固有鍵E1 （Mk 、Ｋｉ）に復号アルゴリズムD1 を施して固有鍵K’ｉ＝D1 （Mk 、E1 （Mk 、Ｋｉ））を生成し（ステップＳ１３２）、乱数発生部３３１は、乱数Ｒ１を生成し（ステップＳ１３３）、通信部３４０は、生成された乱数R1 を通信部２７０を経由して暗号部２５２へ出力し（ステップＳ１３４）、暗号部２５２は、固有鍵Ｋｉを暗号アルゴリズムE2 の鍵として、乱数R1 に暗号アルゴリズムE2 を施して暗号化乱数E2 （Ｋｉ、Ｒ１）を生成し（ステップＳ１３５）、通信部２７０は、通信部３４０を経由して暗号化乱数E2 （Ｋｉ、Ｒ１）を復号部３３３へ出力し（ステップＳ１３６）、復号部３３３は、固有鍵K’ｉを復号アルゴリズムD2 の鍵として、暗号化乱数E2 （Ｋｉ、Ｒ１）に復号アルゴリズムD2 を施して、D2 （K’ｉ、E2 （Ｋｉ、Ｒ１））を生成し（ステップＳ１３７）、相互認証制御部３３４は、乱数R1 とD2 （K’ｉ、E2 （Ｋｉ、Ｒ１））とを比較し、一致していれば、メモリカード２００は正しい装置であると認識し、一致していなければ、メモリカード２００は不正な装置であると認識する（ステップＳ１３８）。

【００５６】

変換部３１１は、マスタ鍵Mk を暗号アルゴリズムE3 の鍵として、装置鍵Ａｊ に暗号アルゴリズムE3 を施して暗号化装置鍵E3 （Mk 、Ａｊ ）を生成し（ステップＳ１３９）、通信部３４０は、暗号化装置鍵E3 （Mk 、Ａｊ ）を通信部２７０を経由して逆変換部２２２へ出力し（ステップＳ１４０）、逆変換部２２２は、マスタ鍵Mk を復号アルゴリズムD3 の鍵として、暗号化装置鍵E3 （Mk 、Ａｊ ）に復号アルゴリズムD3 を施して装置鍵A’ｊ ＝D3 （Mk 、E3 （Mk 、Ａｊ ））を生成し（ステップＳ１４１）、乱数発生部２５１は、乱数R2 を生成し（ステップＳ１４２）、通信部２７０は、生成された乱数R2 を通信部３４０を経由して暗号部３３２へ出力し（ステップＳ１４３）、暗号部３３２は、装置鍵Ａｊ を暗号アルゴリズムE2 の鍵として、乱数R2 に暗号アルゴリズムE2 を施して暗号化乱数E2 （Ａｊ 、R2 ）を生成し（ステップＳ１４４）、通信部３４０は、通信部２７０を経由して暗号化乱数E2 （Ａｊ 、R2 ）を復号部２５３へ出力し（ステップＳ１４５）、復号部２５３は、装置鍵A’ｊ を復号アルゴリズムD2 の鍵として、暗号化乱数E2 （Ａｊ 、R2 ）に復号アルゴリズムD2 を施して、D2 （A’ｊ 、E2 （Ａｊ 、R2 ））を生成し（ステップＳ１４６）、相互認証制御部２５４は、乱数R2 とD2 （A’ｊ 、E2 （Ａｊ 、R2 ））とを比較し、一致していれば、メモリカードライタ３００は正しい装置であると認識し、一致していなければ、メモリカードライタ３００は不正な装置であると認識する（ステップＳ１４７）。

３．その他の実施の形態

なお、本発明を上記の実施の形態に基づいて説明してきたが、本発明は上記の実施の形態に限定されないのはもちろんである。すなわち、以下のような場合も本発明に含まれる。

３．１　デジタル著作物保護システム１００ａ

本発明に係るまた別の実施の形態の一つとしてのデジタル著作物保護システム１００ａは、図１１のブロック図に示すように、メモリカード２００ａ、メディ

ア固有鍵情報作成装置６００、メモリカードライタ３００、メモリカードリーダ４００から構成される。

【００５７】

メモリカードライタ３００、メモリカードリーダ４００は、それぞれデジタル著作物保護システム１００のメモリカードライタ３００、メモリカードリーダ４００とほぼ同様であるので、説明は省略する。

メモリカード２００ａは、メディア固有鍵情報作成装置６００と接続される。

３．１．１　メディア固有鍵情報作成装置６００

メディア固有鍵情報作成装置６００は、マスタ鍵記憶部２１０ｂ、メディア固有鍵記憶部２２０ｂ、変換部２３０ｂ、メディア固有鍵情報記憶部２４０ｂ、通信部２７０ｂから構成される。

【００５８】

マスタ鍵記憶部２１０ｂ、メディア固有鍵記憶部２２０ｂ、変換部２３０ｂ、メディア固有鍵情報記憶部２４０ｂについては、それぞれメモリカード２００のマスタ鍵記憶部２１０、メディア固有鍵記憶部２２０、変換部２３０、メディア固有鍵情報記憶部２４０と同様の機能、作用、構成を有しており、以下においてはそれぞれの相違点を中心にして説明する

（１）マスタ鍵記憶部２１０ｂ

マスタ鍵記憶部２１０ｂは、マスタ鍵記憶部２１０と同様にあらかじめ一つのマスタ鍵Mk を記憶している。

（２）メディア固有鍵記憶部２２０ｂ

メディア固有鍵記憶部２２０ｂは、通信部２７０ｂから固有鍵Ｋｉ を受け取り、受け取った固有鍵Ｋｉ を記憶する。

（３）変換部２３０ｂ

変換部２３０ｂは、変換部２３０と同様にして、メディア固有鍵記憶部２２０

ｂに記憶されている固有鍵Ｋｉ とマスタ鍵記憶部２１０ａに記憶されているマスタ鍵Mk を用いて、暗号化固有鍵Ｊｉ を生成し、生成した暗号化固有鍵Ｊｉ をメディア固有鍵情報記憶部２４０ｂへ出力する。

（４）メディア固有鍵情報記憶部２４０ｂ

メディア固有鍵情報記憶部２４０ｂは、変換部２３０ｂから、暗号化固有鍵Ｊｉ を受け取り、受け取った暗号化固有鍵Ｊｉ を記憶する。

（５）通信部２７０ｂ

通信部２７０ｂは、メモリカード２００ａの通信部２７０ａから固有鍵Ｋｉ を受け取り、受け取った固有鍵Ｋｉ をメディア固有鍵記憶部２２０ｂへ出力する。

【００５９】

通信部２７０ｂは、メディア固有鍵情報記憶部２４０ｂから暗号化固有鍵Ｊｉ を読み出し、読み出した暗号化固有鍵Ｊｉ をメモリカード２００ａの通信部２７０ａへ出力する。

３．１．２　メモリカード２００ａ

メモリカード２００ａは、この図に示すように、マスタ鍵記憶部２１０、メディア固有鍵記憶部２２０、メディア固有鍵情報記憶部２４０ａ、装置鍵記憶部２２１、逆変換部２２２、装置鍵情報記憶部２２３、相互認証部２５０、暗号化著作物記憶部２６０、通信部２７０ａ、制御部２８０から構成される。

【００６０】

メモリカード２００ａのマスタ鍵記憶部２１０、メディア固有鍵記憶部２２０、装置鍵記憶部２２１、逆変換部２２２、装置鍵情報記憶部２２３、相互認証部２５０、暗号化著作物記憶部２６０、制御部２８０は、それぞれ、メモリカード２００のマスタ鍵記憶部２１０、メディア固有鍵記憶部２２０、装置鍵記憶部２２１、逆変換部２２２、装置鍵情報記憶部２２３、相互認証部２５０、暗号化著作物記憶部２６０、制御部２８０と同じであるので説明を省略し、メモリカード２００ａのメディア固有鍵情報記憶部２４０ａ、通信部２７０ａについて、メモ

リカード２００のメディア固有鍵情報記憶部２４０、通信部２７０との相違点を中心にして説明する。

（１）メディア固有鍵情報記憶部２４０ａ

メディア固有鍵情報記憶部２４０ａは、通信部２７０ａから暗号化固有鍵Ｊｉを受け取り、受け取った暗号化固有鍵Ｊｉ を記憶する。

（２）通信部２７０ａ

通信部２７０ａは、メディア固有鍵記憶部２２０から固有鍵Ｋｉ を読み出し、読み出した固有鍵Ｋｉ をメディア固有鍵情報作成装置６００の通信部２７０ｂへ出力する。

【００６１】

通信部２７０ａは、メディア固有鍵情報作成装置６００の通信部２７０ｂから暗号化固有鍵Ｊｉ を受け取り、受け取った暗号化固有鍵Ｊｉ をメディア固有鍵情報記憶部２４０ａへ出力する。

３．１．３　メモリカード２００ａがメモリカードライタ３００に装着された場合の詳細の認証動作

メモリカード２００ａが、メモリカードライタ３００に装着された場合の詳細の認証動作について、図９との相違点につき、図１２を用いて説明する。

【００６２】

認証動作の詳細は、図９に示すステップＳ１３９～Ｓ１４７が、図１２に示すステップＳ２０１～Ｓ２０６に置き換えられたものとなる。

乱数発生部２５１は、乱数Ｒ3 を生成し（ステップＳ２０１）、通信部２７０ａは、生成された乱数Ｒ3 を通信部３４０を経由して暗号部３３２へ出力し（ステップＳ２０２）、暗号部３３２は、マスタ鍵Mk を暗号アルゴリズムＥ2 の鍵として、乱数Ｒ3 に暗号アルゴリズムＥ2 を施して暗号化乱数Ｅ2 （Mk 、Ｒ3 ）を生成し（ステップＳ２０３）、通信部３４０は、通信部２７０を経由して暗号化乱数Ｅ2 （Mk 、Ｒ3 ）を復号部２５３へ出力し（ステップＳ２０４）、復

号部２５３は、マスタ鍵Mk を復号アルゴリズムD2 の鍵として、暗号化乱数Ｅ２（Mk 、Ｒ３）に復号アルゴリズムD2 を施して、D2（Mk 、E2（Mk 、R3））を生成し（ステップＳ２０５）、相互認証制御部２５４は、乱数Ｒ３とD2（Mk 、E2（Mk 、R3））とを比較し、一致していれば、メモリカードライタ３００は正しい装置であると認識し、一致していなければ、メモリカードライタ３００は不正な装置であると認識する（ステップＳ２０６）。

３．１．４　まとめ

この実施の形態によると、メモリカード２００ａが使用者に配布、販売される前に、メモリカード２００ａとメディア固有鍵情報作成装置６００とが接続され、メディア固有鍵情報作成装置６００により生成された暗号化固有鍵Ｊｉ がメモリカード２００ａに書き込まれる。

【００６３】

このように構成することにより、メモリカード２００から、変換部２３０を取り去ることができ、メモリカード２００ａでは、メモリカード２００と比較して回路規模を小さくできるという効果がある。

３．２　別のデジタル著作物保護システム

デジタル著作物保護システム１００では、メモリカード２００、メモリカードライタ３００、メモリカードリーダ４００は、同一のマスタ鍵を有し、マスタ鍵を共通鍵暗号アルゴリズム又は共通鍵復号アルゴリズムの鍵としているが、マスタ鍵の代わりに、メモリカード２００は公開鍵暗号の一種であるＲＳＡ暗号の公開鍵Kp を有し、メモリカードライタ３００、メモリカードリーダ４００は、その秘密鍵Ks を有するとしてもよい。

【００６４】

ここで、公開鍵Kp と秘密鍵Ks は、次のようにして決定される。ｐ、ｑをそれぞれ約１６０桁程度の１０進数とし、その積をｎとし、整数Ｌをｐ－１及びｑ－１の最小公倍数とし、数ｅ及びｄを法Ｌの下で互いに逆数となる数とする。すなわち、ｅ・ｄ＝１（ｍｏｄ－Ｌ）とする。また、公開鍵Kp をｎ及びｅとし、

秘密鍵Ｋｓ をｄとする。変換部においては、入力Ｍに対して法ｎの下でＭ＾ｅ（Ｍのｅ乗）の演算を行って変換結果Ｃを求め、逆変換部においては、入力Ｃに対してＣ＾ｄ（Ｃのｄ乗）の演算を行う。法ｎの下でＣ＾ｄ＝（Ｍ＾ｅ）＾ｄ＝Ｍ＾ｅｄ＝Ｍであるから首尾よく逆変換ができることが分かる。

【００６５】

公開鍵Ｋｐ は、上記に示すようにしてあらかじめ別の公開鍵生成装置により生成され、生成された公開鍵Ｋｐ がメモリカード２００に送信されている。

（メモリカード２００がメモリカードライタ３００に装着された場合の詳細の認証動作）

次に、メモリカード２００がメモリカードライタ３００に装着された場合の詳細の認証動作について図１３を用いて説明する。なお、図１０と同じ符号を有するステップについては、同じ動作であるので説明を省略する。

【００６６】

公開鍵生成装置は、あらかじめメモリカードライタ３００から秘密鍵Ｋｓ を読み出し、読み出した秘密鍵Ｋｓ を基にして公開鍵暗号アルゴリズムを用いて、公開鍵Ｋｐ を生成し、生成した公開鍵Ｋｐ をメモリカード２００に送信し、メモリカード２００は送信された公開鍵Ｋｐ を記憶する（ステップＳ３０１）。

変換部２３０は、公開鍵Ｋｐ を暗号アルゴリズムＥ4 の鍵として、固有鍵Ｋｉに暗号アルゴリズムＥ4 を施して暗号化固有鍵Ｅ4 （Ｋｐ、Ｋｉ）を生成し（ステップＳ３０２）、通信部２７０は、暗号化固有鍵Ｅ4 （Ｋｐ、Ｋｉ）を通信部３４０を経由して逆変換部３２１へ出力し（ステップＳ３０３）、逆変換部３２１は、秘密鍵Ｋｓ を復号アルゴリズムＤ4 の鍵として、暗号化固有鍵Ｅ4 （Ｋｐ、Ｋｉ）に復号アルゴリズムＤ4 を施して固有鍵Ｋ’ｉ＝Ｄ4 （Ｋｓ、Ｅ4 （Ｋｐ、Ｋｉ））を生成する（ステップＳ３０４）。

【００６７】

なお、暗号アルゴリズムＥ4 及び復号復号アルゴリズムＤ4 は楕円暗号によるアルゴリズムである。

公開鍵と秘密鍵がこのように構成されているため、秘密鍵ｄから公開鍵ｅを計算できない。なぜならば、秘密鍵ｄが分かっているとき、これからｅを求めるた

めには法Ｌが知られていなければならないが、Ｌはｐ－１とｑ－１の最小公倍数であるため、ｐとｑとの積を知っているだけでは求められないからである。このことにより、カードリーダ又はカードライタに存在する秘密鍵ｄが仮に暴露されたとしてもこれから公開鍵ｅを求めることができないので、メモリカードの偽造が困難であるという効果がある。

３．３　別のデジタル著作物保護システム

上記の「３．２　別のデジタル著作物保護システム」に示すデジタル著作物保護システムでは、メモリカード２００は公開鍵Ｋｐ を有し、メモリカードライタ３００、メモリカードリーダ４００は、秘密鍵Ｋｓ を有するとしているが、また別のデジタル著作物保護システムにおいては、メモリカード２００は、公開鍵暗号系の一種である楕円曲線上の回復型署名の秘密鍵Ｋｓ を有し、メモリカードライタ３００、メモリカードリーダ４００は、公開鍵Ｋｐ を有するとしてもよい。ここで、公開鍵Ｋｐ と秘密鍵Ｋｓ は次のようにして決定される。

【００６８】

秘密鍵Ｋｓ としてスカラーｘが選ばれる。公開鍵Ｋｐ は、楕円曲線上の基点をＧとし、Ｇ＋Ｇ＋・・・＋Ｇ（ｘ回の加算）の点とする。変換処理として秘密鍵Ｋｓ を用いた回復型署名変換を用い、逆変換処理として公開鍵Ｋｐ を用いて回復型署名検証変換を用いる。なお、回復型署名については、「A message recovery signature scheme equivalent to DSA over elliptic curves」(Atsuko Miyaji 著、Advances in Cryptology- Proceedings of ASIACRYPT'96,Lecture Notes in Computer Science,1163(1996),Springer-Verlag,1-14 ）に記載されているので、説明は省略する。

【００６９】

このとき、公開鍵Ｋｐ は、メモリカード２００が有する秘密鍵Ｋｓ を基にして公開鍵暗号アルゴリズムを用いて、あらかじめ別の公開鍵生成装置により生成され、生成された公開鍵Ｋｐ がメモリカードライタ３００に送信されている。

変換部２３０は、秘密鍵Ｋｓ を暗号アルゴリズムＥ４ の鍵として、固有鍵Ｋｉ に暗号アルゴリズムＥ４ を施して暗号化固有鍵Ｅ４ （Ｋｓ 、Ｋｉ ）を生成する。

また、逆変換部３２１は、公開鍵Ｋｐ を復号アルゴリズムＤ4 の鍵として、暗号化固有鍵Ｅ4 （Ｋｓ 、Ｋｉ ）に復号アルゴリズムＤ4 を施して固有鍵Ｋ’ｉ ＝Ｄ4 （Ｋｐ 、Ｅ4 （Ｋｓ 、Ｋｉ ））を生成する。

【００７０】

公開鍵Ｋｐ と秘密鍵Ｋｓ がこのように構成されているので、公開鍵Ｋｐ から秘密鍵Ｋｓ を求めることが、計算量的に非常に困難となる。従って、メモリカードに比べて内部解析の危険性が相対的に高いと思われるメモリライタ又はメモリリーダに公開鍵を与え、メモリカードに秘密鍵を与える構成が、全体のセキャリティを高める効果を持つ。

【００７１】

なお、楕円曲線暗号系のような離散対数問題に安全性の根拠を持つ公開鍵暗号系では、秘密鍵から公開鍵が求められることに注意されたい。

３．４　別のデジタル著作物保護システム

本発明に係るまた別の実施の形態の一つとしてのデジタル著作物保護システム１００ｃは、図１４、図１５、図１６のブロック図にそれぞれ示すメモリカード２００ｃ、メモリカードライタ３００ｃ、メモリカードリーダ４００ｃから構成される。

【００７２】

メモリカード２００ｃは、図示していないマスタ鍵選択装置に装着される。また、メモリカードライタ３００ｃ、メモリカードリーダ４００ｃは、マスタ鍵選択装置に接続される。

３．４．１　マスタ鍵選択装置

マスタ鍵選択装置にメモリカード２００ｃが装着される場合には、マスタ鍵選択装置は、メモリカード２００ｃの通信部２７０と接続される。

【００７３】

マスタ鍵選択装置とメモリカードライタ３００ｃとが接続される場合には、マスタ鍵選択装置は、メモリカードライタ３００ｃの通信部３４０と接続される。

マスタ鍵選択装置とメモリカードリーダ４００ｃとが接続される場合には、マスタ鍵選択装置は、メモリカードリーダ４００ｃの通信部４４０と接続される。

マスタ鍵選択装置は、メモリカード２００ｃ、メモリカードライタ３００ｃ又はメモリカードリーダ４００ｃと接続される場合に、接続されるメモリカード２００ｃの通信部２７０、メモリカードライタ３００ｃの通信部３４０又はメモリカードリーダ４００ｃの通信部４４０に対してパスワードを出力する。

【００７４】

パスワードは、複数のマスタ鍵のうちの一つに対応する。

３．４．２　メモリカード２００ｃ

メモリカード２００ｃは、メモリカード２００にさらにマスタ鍵選択部２１５を備える。メモリカード２００ｃのその他の構成要素は、メモリカード２００と同様である。以下において、メモリカード２００との相違点を中心にして説明する。

【００７５】

マスタ鍵記憶部２１０は、複数のマスタ鍵をあらかじめ記憶している。

メモリカード２００ｃがマスタ鍵選択装置に装着されたとき、メモリカード２００ｃは、マスタ鍵選択装置と通信部２７０を介して接続される。

通信部２７０は、マスタ鍵選択装置からパスワードを受け取り、受け取ったパスワードをマスタ鍵選択部２１５に出力する。

【００７６】

マスタ鍵選択部２１５は、通信部２７１から受け取ったパスワードを用いて、対応する一つのマスタ鍵をマスタ鍵記憶部２１０から選択し、選択したマスタ鍵をマスタ鍵記憶部２１０へ出力する。

マスタ鍵記憶部２１０は、選択されたマスタ鍵に選択されたことを示す選択マークを付し、記憶する。

【００７７】

変換部２０３、逆変換部２２２は、前記選択マークを付されたマスタ鍵を読み出す。

３．４．３　メモリカードライタ３００ｃ、メモリカードリーダ４００ｃ

メモリカードライタ３００ｃは、メモリカードライタ３００にさらにマスタ鍵選択部３１５を備える。メモリカードライタ３００ｃのその他の構成要素は、メモリカードライタ３００と同様である。

【００７８】

マスタ鍵記憶部３１３は、複数のマスタ鍵をあらかじめ記憶している。

メモリカード２００ｃと同様に、通信部３４０はマスタ鍵選択装置からパスワードを受け取り、マスタ鍵選択部３１５に出力し、マスタ鍵選択部３１５は、受け取ったパスワードを用いて、対応する一つのマスタ鍵をマスタ鍵記憶部３１３から選択し、マスタ鍵記憶部３１３は、選択されたマスタ鍵に選択されたことを示す選択マークを付し、記憶する。

【００７９】

変換部３１１、逆変換部３２１は、前記選択マークを付されたマスタ鍵を読み出す。

メモリカードリーダ４００ｃについても、メモリカードライタ３００ｃと同様である。

３．４．４　まとめ

本実施の形態が適用される望ましい運用形態においては、運用システムの規格を決定すると同時にマスタ鍵などの秘密情報の秘密性を確保する立場にあり、各製造業者にライセンスの許諾を与えるライセンス組織と、ライセンス組織より許諾を受け、所定の規格の機器を製造し、ユーザに提供する立場にある製造業者と、個々の機器を利用するユーザとの３者が存在する。メモリカード用のマスタ鍵選択装置９０１とメモリカードライタ用のマスタ鍵選択装置９０２とメモリカードリーダ用のマスタ鍵選択装置９０３とのうち、マスタ鍵選択装置９０１は製造業者の手元にあり、マスタ鍵選択装置９０２とマスタ鍵選択装置９０３とはライセンス組織の手元にあって、製造業者には渡されない。

【００８０】

従って、製造業者が製造する装置の運用状態においては、メモリカードは複数のマスタ鍵を有しており、そのうちの一つをマスタ鍵選択装置９０１により選択する。一方、メモリカードライタ又はメモリカードリーダには、予めライセンス組織がマスタ鍵選択装置９０１又は９０２を用いて選択した結果のマスタ鍵だけが記録されている。

【００８１】

マスタ鍵は運用システム毎に選ばれる。例えば、Ａ社、Ｂ社、Ｃ社の３者が共同で運営する音楽配信システムには、マスタ鍵Mk1が用いられ、Ｘ社、Ｙ社、Ｚ社が共同で運営する映画レンタルシステムにはマスタ鍵Mk2が用いられる。

このように、装置の製造に当たって厳重なセキュリティ条件を課すことが困難なため、異なる運用システムに異なるマスタ鍵が用いられるので、メモリカードよりも相対的に解析が容易と思われるメモリカードライタ又はメモリカードリーダを運用システム毎に特化することにより、ある運用システムのマスタ鍵の暴露が他の運用システムに影響を与えない、安全性の高いセキュリティシステムを実現できるという効果がある。

３．５　その他の変形例

（１）上記の実施の形態においては、デジタル著作物保護システムは、メモリカードとメモリメモリカードライタとメモリカードリーダとから構成されるとしているが、デジタル著作物保護システムは、メモリカードとメモリカードライタとから構成されるとしてもよい。また、デジタル著作物保護システムは、メモリカードとメモリカードリーダとから構成されるとしてもよい。

（２）上記の実施の形態においては、ＤＥＳ暗号を用いるとしているが他の暗号を用いてもよい。

（３）メモリカードは、半導体メモリの代わりに、光ディスク媒体やＭＯ（Ｍａｇｎｅｔｏ－Ｏｐｔｉｃａｌ）媒体を有するとしてもよい。

（４）本発明は、コンピュータにより実行するプログラムを記録したコンピュータ読み取り可能な記録媒体であって、上記手順をコンピュータに実行させるプログラムを記録していることを特徴とする。

（５）また、前記記録媒体を移送することにより、又は、前記プログラムを通信回線を通して移送することにより、独立した他のコンピュータシステムで実施するようにしてもよい。

【００８２】

【発明の効果】

上記に説明したように、本発明は、記録媒体とアクセス装置とが接続された状態で、両者間で機器認証フェーズと著作物転送フェーズとを実行して著作物の正当者への配布を実現するデジタル著作物保護システムであって、機器認証フェーズでは、記録媒体が所有する固有鍵をアクセス装置に秘密伝送し、アクセス装置が取得した固有鍵を用いて、機器認証を行い、著作物転送フェーズでは、機器認証が成功した場合にのみ、アクセス装置が取得した固有鍵を用いて著作物を暗号化して記録媒体に転送し若しくは記録媒体から転送された著作物を復号する。

【００８３】

この構成によると、適正なアクセス装置が行った認証の手順を模倣する不正な記録装置のリプレイ攻撃に耐えうる強固な認証処理を実現することができるという効果がある。また、不正な装置が適正な装置を欺いて、著作物を不正に読み出し又は著作物を不正に書き込むことを防ぐことができるという効果がある。

また、本発明は、記録媒体とアクセス装置とが接続された状態で、前記記録媒体と前記アクセス装置との間で機器認証と暗号化された著作物の転送とを行うデジタル著作物保護システムであって、前記記録媒体は、記録媒体毎に異なる固有鍵を予め記憶している固有鍵記憶領域と、接続されたアクセス装置へ前記固有鍵を秘密伝送し、前記固有鍵を用いて前記アクセス装置との間で機器認証を行う第１認証手段と、前記固有鍵を用いて暗号化される著作物を保持するための領域とを備え、前記アクセス装置は、記録媒体から秘密伝送された固有鍵を用いて、前記記録媒体との間で機器認証を行う第２認証手段と、機器認証が成功した場合にのみ、前記機器認証を経て得た固有鍵を用いて著作物を暗号化して記録媒体に転送し若しくは記録媒体から転送された著作物を復号する転送手段とを備える。

【００８４】

この構成によると、適正なアクセス装置が行った認証の手順を模倣する不正な記録装置のリプレイ攻撃に耐えうる強固な認証処理を実現することができるという効果がある。また、不正な装置が適正な装置を欺いて、著作物を不正に読み出し又は著作物を不正に書き込むことを防ぐことができるという効果がある。

ここで、前記第１認証手段は、あらかじめ第１鍵を有し、前記第１鍵を用いて、前記固有鍵に第１暗号を施して暗号化固有鍵を生成して伝送し、前記第２認証手段は、あらかじめ前記第１鍵を有し、前記第１鍵を用いて、前記伝送された暗号化固有鍵に、前記第１暗号の逆変換を行う第１復号を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器認証を行い、前記転送手段は、前記復号固有鍵を用いて著作物の転送を行うように構成してもよい。

【００８５】

この構成によると、記録装置とアクセス装置とは同一のマスタ鍵を有するので、記録装置とアクセス装置との製造が容易に行えるという効果がある。

ここで、前記第１認証手段は、第１鍵を基にして、公開鍵暗号方式の公開鍵決定アルゴリズムにより算出された公開鍵である第２鍵をあらかじめ有し、前記第２鍵を用いて、前記固有鍵に第１暗号を施して暗号化固有鍵を生成して伝送し、前記第２認証手段は、あらかじめ前記第１鍵を有し、前記第１鍵を用いて、前記伝送された暗号化固有鍵に、前記第１暗号の逆変換を行う第１復号を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器認証を行い、前記転送手段は、前記復号固有鍵を用いて著作物の転送を行うように構成してもよい。

【００８６】

この構成によると、秘密鍵ｄから公開鍵ｅを計算できない。なぜならば、秘密鍵ｄが分かっているとき、これからｅを求めるためには法Ｌが知られていなければならないが、Ｌはｐ－１とｑ－１の最小公倍数であるため、ｐとｑとの積を知っているだけでは求められないからである。このことにより、カードリーダ又は

カードライタに存在する秘密鍵ｄが仮に暴露されたとしてもこれから公開鍵ｅを求めることができないので、メモリカードの偽造が困難であるという効果がある。

ここで、前記第１認証手段は、あらかじめ第１鍵を有し、前記第１鍵を用いて、前記固有鍵に回復型署名処理を施して署名文を生成して伝送し、前記第２認証手段は、前記第１鍵に前記回復型署名処理の公開鍵決定アルゴリズムにより算出された公開鍵である第２鍵をあらかじめ有し、前記第２鍵を用いて、前記伝送された署名文に、前記回復型署名の検証処理を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器認証を行い、前記転送手段は、前記復号固有鍵を用いて著作物の転送を行うように構成してもよい。

【００８７】

この構成によると、公開鍵Ｋｐ から秘密鍵Ｋｓ を求めることが、計算量的に非常に困難となる。従って、メモリカードに比べて内部解析の危険性が相対的に高いと思われるメモリライタ又はメモリリーダに公開鍵を与え、メモリカードに秘密鍵を与える構成が、全体のセキャリティを高めると言う効果がある。

ここで、前記デジタル著作物保護システムは、さらに固有鍵に第１暗号を施して暗号化固有鍵に変換する固有鍵変換手段を備える暗号化固有鍵作成装置を有し、前記第１認証手段は、前記固有鍵を前記固有鍵変換手段へ出力して暗号化固有鍵に変換し、変換された暗号化固有鍵を前記アクセス装置へ伝送し、前記第２認証手段は、記録媒体から伝送された暗号化固有鍵に前記第１暗号の逆処理を行う第１復号を施して固有鍵を生成するように構成してもよい。

【００８８】

この構成によると、記録媒体は、変換部を有しないので、回路規模を小さくすることができるという効果を有する。

ここで、前記第１認証手段は、あらかじめ複数の第１鍵を有し、前記複数の第１鍵のうち一つの第２鍵の選択を受け付け、前記第２鍵を用いて、前記固有鍵に

第１暗号を施して暗号化固有鍵を生成して伝送し、前記第２認証手段は、あらかじめ複数の第１鍵を有し、前記複数の第１鍵から前記第２鍵の選択を受け付け、前記第２鍵を用いて、前記伝送された暗号化固有鍵に、前記第１暗号の逆変換を行う第１復号を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器認証を行い、前記転送手段は、前記復号固有鍵を用いて著作物の転送を行うように構成してもよい。

【００８９】

この構成によると、記録媒体及びアクセス装置は、複数のマスタ鍵を有しているので、複数の異なるデジタル著作物保護システムにおいても適用ができるという効果がある。

また、本発明は、アクセス装置と接続された状態で、前記アクセス装置との間で機器認証と暗号化された著作物の転送とを行う記録媒体であって、記録媒体毎に異なる固有鍵を記憶している固有鍵記憶領域と、前記固有鍵を用いて暗号化される著作物を保持するための領域と、アクセス装置が接続されたとき、記録媒体から当該アクセス装置へ固有鍵を秘密伝送する手順を経て、当該アクセス装置との間で機器認証を行う認証手段と、機器認証が成功した場合にのみ、前記固有鍵を用いて暗号化された著作物を受け取り前記領域に書き込み若しくは前記領域に記憶されている暗号化された著作物を読み出して前記アクセス装置へ出力する転送手段とを備える。

【００９０】

この媒体を用いると、適正なアクセス装置が行った認証の手順を模倣する不正な記録装置のリプレイ攻撃に耐えうる強固な認証処理を実現することができるという効果がある。また、不正な装置が適正な装置を欺いて、著作物を不正に読み出し又は著作物を不正に書き込むことを防ぐことができるという効果がある。

また、本発明は、固有鍵を有する記録媒体と接続され、前記記録媒体との間で機器認証と暗号化された著作物の転送とを行うアクセス装置であって、記録媒体から固有鍵を秘密伝送される手順を経て、前記記録媒体との間で機器認証を行う

認証手段と、機器認証が成功した場合にのみ、前記機器認証を経て得た固有鍵を用いて著作物を暗号化して記録媒体に転送し若しくは記録媒体から転送された著作物を復号する転送手段とを備える。

【００９１】

このアクセス装置を用いると、適正なアクセス装置が行った認証の手順を模倣する不正な記録装置のリプレイ攻撃に耐えうる強固な認証処理を実現することができるという効果がある。また、不正な装置が適正な装置を欺いて、著作物を不正に読み出し又は著作物を不正に書き込むことを防ぐことができるという効果がある。

また、本発明は、記録媒体とアクセス装置とが接続された状態で、両者間で機器認証ステップと著作物転送ステップとを実行して著作物の正当者への配布を実現するデジタル著作物保護方法であって、機器認証ステップでは、記録媒体が所有する固有鍵をアクセス装置に秘密伝送し、アクセス装置が取得した固有鍵を用いて、機器認証を行い、著作物転送ステップでは、機器認証が成功した場合にのみ、アクセス装置が取得した固有鍵を用いて著作物を暗号化して記録媒体に転送し若しくは記録媒体から転送された著作物を復号する。

【００９２】

この方法を用いると、適正なアクセス装置が行った認証の手順を模倣する不正な記録装置のリプレイ攻撃に耐えうる強固な認証処理を実現することができるという効果がある。また、不正な装置が適正な装置を欺いて、著作物を不正に読み出し又は著作物を不正に書き込むことを防ぐことができるという効果がある。

また、本発明は、記録媒体毎に異なる固有鍵を予め記憶している固有鍵記憶領域及び前記固有鍵を用いて暗号化される著作物を保持するための領域を有する記録媒体とアクセス装置とが接続された状態で、前記記録媒体と前記アクセス装置との間で機器認証と暗号化された著作物の転送とを行うデジタル著作物保護システムで用いられるデジタル著作物保護方法であって、接続されたアクセス装置へ

前記固有鍵を秘密伝送し、前記固有鍵を用いて前記アクセス装置との間で機器認証を行う第１認証ステップと、記録媒体から秘密伝送された固有鍵を用いて、前記記録媒体との間で機器認証を行う第２認証ステップと、機器認証が成功した場合にのみ、前記機器認証を経て得た固有鍵を用いて著作物を暗号化して記録媒体に転送し若しくは記録媒体から転送された著作物を復号する転送ステップとを含む。

【００９３】

この方法を用いると、適正なアクセス装置が行った認証の手順を模倣する不正な記録装置のリプレイ攻撃に耐えうる強固な認証処理を実現することができるという効果がある。また、不正な装置が適正な装置を欺いて、著作物を不正に読み出し又は著作物を不正に書き込むことを防ぐことができるという効果がある。

ここで、前記第１認証ステップは、あらかじめ第１鍵を有し、前記第１鍵を用いて、前記固有鍵に第１暗号を施して暗号化固有鍵を生成して伝送し、前記第２認証ステップは、あらかじめ前記第１鍵を有し、前記第１鍵を用いて、前記伝送された暗号化固有鍵に、前記第１暗号の逆変換を行う第１復号を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器認証を行い、前記転送ステップは、前記復号固有鍵を用いて著作物の転送を行うように構成してもよい。

【００９４】

この方法を用いると、記録装置とアクセス装置とは同一のマスタ鍵を有するので、記録装置とアクセス装置との製造が容易に行えるという効果がある。

ここで、前記第１認証ステップは、第１鍵を基にして、公開鍵暗号方式の公開鍵決定アルゴリズムにより算出された公開鍵である第２鍵をあらかじめ有し、前記第２鍵を用いて、前記固有鍵に第１暗号を施して暗号化固有鍵を生成して伝送し、前記第２認証ステップは、あらかじめ前記第１鍵を有し、前記第１鍵を用いて、前記伝送された暗号化固有鍵に、前記第１暗号の逆変換を行う第１復号を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器

認証を行い、前記転送ステップは、前記復号固有鍵を用いて著作物の転送を行うように構成してもよい。

【００９５】

この方法を用いると、秘密鍵ｄから公開鍵ｅを計算できない。なぜならば、秘密鍵ｄが分かっているとき、これからｅを求めるためには法Ｌが知られていなければならないが、Ｌはｐ－１とｑ－１の最小公倍数であるため、ｐとｑとの積を知っているだけでは求められないからである。このことにより、カードリーダ又はカードライタに存在する秘密鍵ｄが仮に暴露されたとしてもこれから公開鍵ｅを求めることができないので、メモリカードの偽造が困難であるという効果がある。

ここで、前記第１認証ステップは、あらかじめ第１鍵を有し、前記第１鍵を用いて、前記固有鍵に回復型署名処理を施して署名文を生成して伝送し、前記第２認証ステップは、前記第１鍵に前記回復型署名処理の公開鍵決定アルゴリズムにより算出された公開鍵である第２鍵をあらかじめ有し、前記第２鍵を用いて、前記伝送された署名文に、前記回復型署名の検証処理を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器認証を行い、前記転送ステップは、前記復号固有鍵を用いて著作物の転送を行うように構成してもよい。

【００９６】

この方法を用いると、公開鍵Ｋｐ から秘密鍵Ｋｓ を求めることが、計算量的に非常に困難となる。従って、メモリカードに比べて内部解析の危険性が相対的に高いと思われるメモリライタ又はメモリリーダに公開鍵を与え、メモリカードに秘密鍵を与える構成が、全体のセキャリティを高めると言う効果がある。

ここで、前記デジタル著作物保護システムは、さらに固有鍵に第１暗号を施して暗号化固有鍵に変換する固有鍵変換手段を備える暗号化固有鍵作成装置を有し、前記第１認証ステップは、前記固有鍵を前記固有鍵変換手段へ出力して暗号化固有鍵に変換し、変換された暗号化固有鍵を前記アクセス装置へ伝送し、前記第２認証ステップは、記録媒体から伝送された暗号化固有鍵に前記第１暗号の逆処

理を行う第１復号を施して固有鍵を生成するように構成してもよい。

【００９７】

この方法を用いると、記録媒体は、変換部を有しないので、回路規模を小さくすることができるという効果を有する。

ここで、前記第１認証ステップは、あらかじめ複数の第１鍵を有し、前記複数の第１鍵のうち一つの第２鍵の選択を受け付け、前記第２鍵を用いて、前記固有鍵に第１暗号を施して暗号化固有鍵を生成して伝送し、前記第２認証ステップは、あらかじめ複数の第１鍵を有し、前記複数の第１鍵から前記第２鍵の選択を受け付け、前記第２鍵を用いて、前記伝送された暗号化固有鍵に、前記第１暗号の逆変換を行う第１復号を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器認証を行い、前記転送ステップは、前記復号固有鍵を用いて著作物の転送を行うように構成してもよい。

【００９８】

この方法を用いると、記録媒体及びアクセス装置は、複数のマスタ鍵を有しているので、複数の異なるデジタル著作物保護システムにおいても適用ができるという効果がある。

また、本発明は、以上に説明したデジタル著作物保護方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体であり、前記プログラムにより上記方法をコンピュータに実行させることにより、上記デジタル著作物保護システムと同様の効果を奏することは明らかである。

【図面の簡単な説明】

【図１】

本発明に係る一つの実施の形態としてのデジタル著作物保護システム１００のブロック図を示す。

【図２】

メモリカード２００がメモリカードライタ３００に装着され、メモリカードライタ３００がパーソナルコンピュータ５００に装着される状態を示す。

【図３】

メモリカード２００がメモリカードリーダ４００の一種であるヘッドホンステレオ４０１に装着される状態を示す。

【図４】

メモリカード２００の構成を示すブロック図である。

【図５】

メモリカードライタ３００の構成を示すブロック図である。

【図６】

メモリカードリーダ４００の構成を示すブロック図である。

【図７】

メモリカード２００が、メモリカードライタ３００に装着された場合の概要動作を示すフローチャートである。

【図８】

メモリカード２００が、メモリカードリーダ４００に装着された場合の概要動作を示すフローチャートである。

【図９】

メモリカード２００が、メモリカードライタ３００に装着された場合の詳細の認証動作を示す。

【図１０】

メモリカード２００が、メモリカードライタ３００に装着された場合の詳細の認証動作を示す。

【図１１】

本発明に係るまた別の実施の形態の一つとしてのデジタル著作物保護システム１００ａの構成を示すブロック図である。

【図１２】

メモリカード２００ａが、メモリカードライタ３００に装着された場合の詳細の認証動作を示す。

【図１３】

本発明に係るまた別の実施の形態の一つとしてのデジタル著作物保護システム

において、メモリカード２００がメモリカードライタ３００に装着された場合の詳細の認証動作を示す。

【図１４】

本発明に係るまた別の実施の形態の一つとしてのデジタル著作物保護システム１００ｃにおけるメモリカード２００ｃの構成を示すブロック図である。

【図１５】

デジタル著作物保護システム１００ｃにおけるメモリカードライタ３００ｃの構成を示すブロック図である。

【図１６】

デジタル著作物保護システム１００ｃにおけるメモリカードリーダ４００ｃの構成を示すブロック図である。

【符号の説明】

１０　通信回線
１００　デジタル著作物保護システム
２００　メモリカード
２１０　マスタ鍵記憶部
２２０　メディア固有鍵記憶部
２２１　装置鍵記憶部
２２２　逆変換部
２２３　装置鍵情報記憶部
２３０　変換部
２４０　メディア固有鍵情報記憶部
２５０　相互認証部
２５１　乱数発生部
２５２　暗号部
２５３　復号部
２５４　相互認証制御部２５４
２６０　暗号化著作物記憶部
２７０　通信部

２８０　制御部

３００　メモリカードライタ

３１０　装置鍵記憶部

３１１　変換部

３１２　装置鍵情報記憶部

３１３　マスタ鍵記憶部

３２０　メディア固有鍵情報記憶部

３２１　逆変換部

３２３　メディア固有鍵記憶部

３３０　相互認証部

３３１　乱数発生部

３３２　暗号部

３３３　復号部

３３４　相互認証制御部

３４０　通信部

３５０　制御部

３６０　暗号部

３７０　著作物記憶部

３８０　著作物取得部

４００　メモリカードリーダ

４１０　装置鍵記憶部

４１１　変換部

４１２　装置鍵情報記憶部

４１３　マスタ鍵記憶部

４２０　メディア固有鍵情報記憶部

４２１　逆変換部

４２３　メディア固有鍵記憶部

４３０　相互認証部

４３１　乱数発生部

４３２　暗号部

４３３　復号部

４３４　相互認証制御部

４４０　通信部

４５０　制御部

４６０　復号部

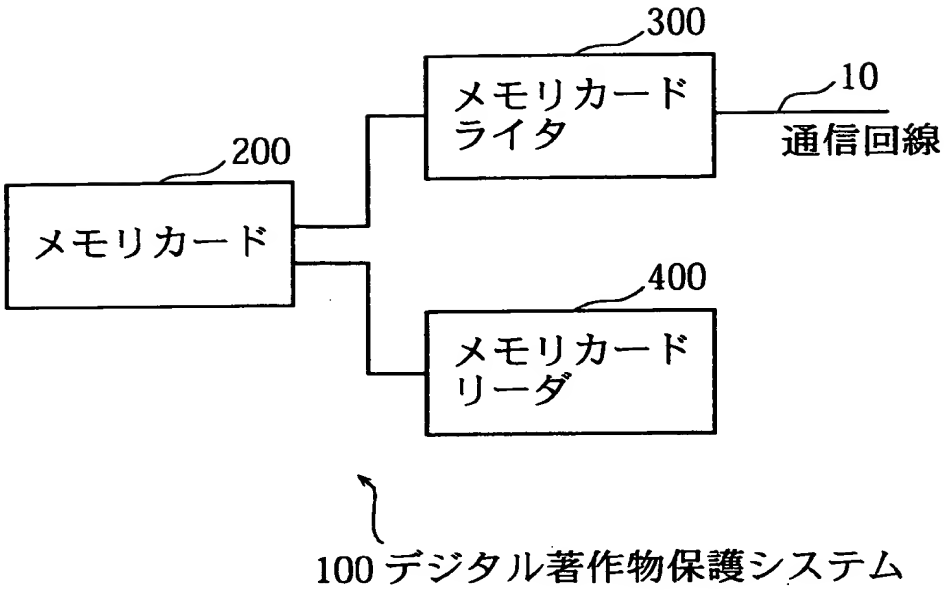
４７０　著作物記憶部

４８０　再生部

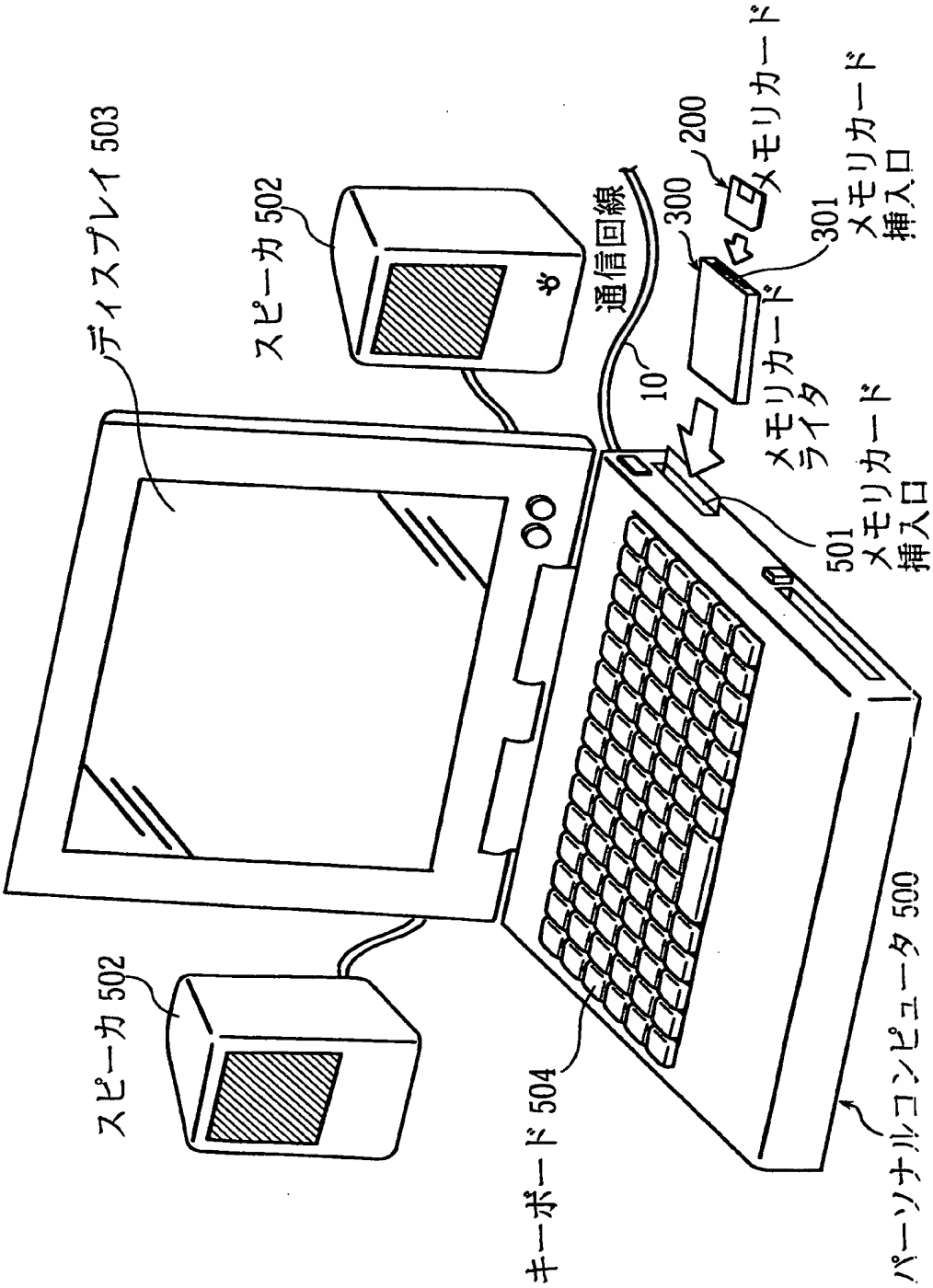
４９０　操作部

【書類名】　　図面

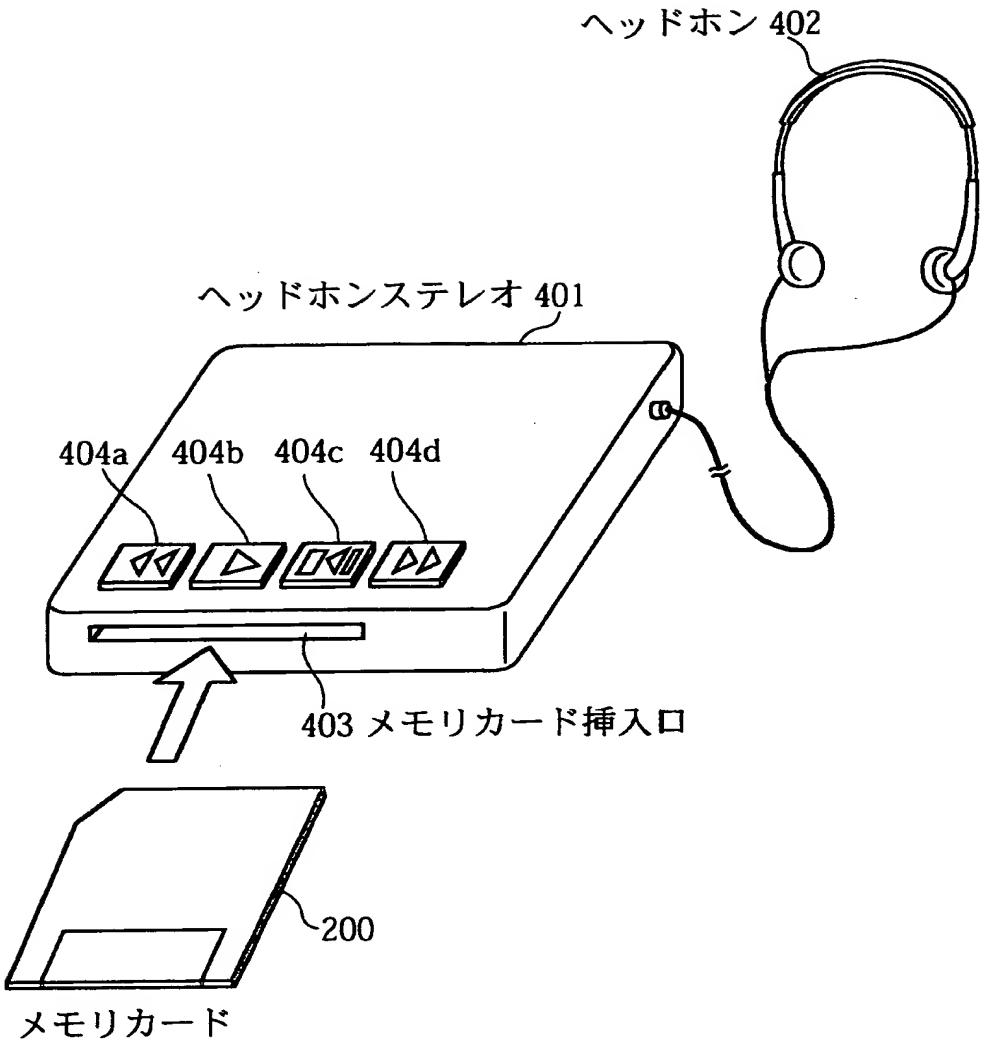
【図１】


300
メモリカード
ライタ
10
通信回線
200
メモリカード
400
メモリカード
リーダ
100 デジタル著作物保護システム

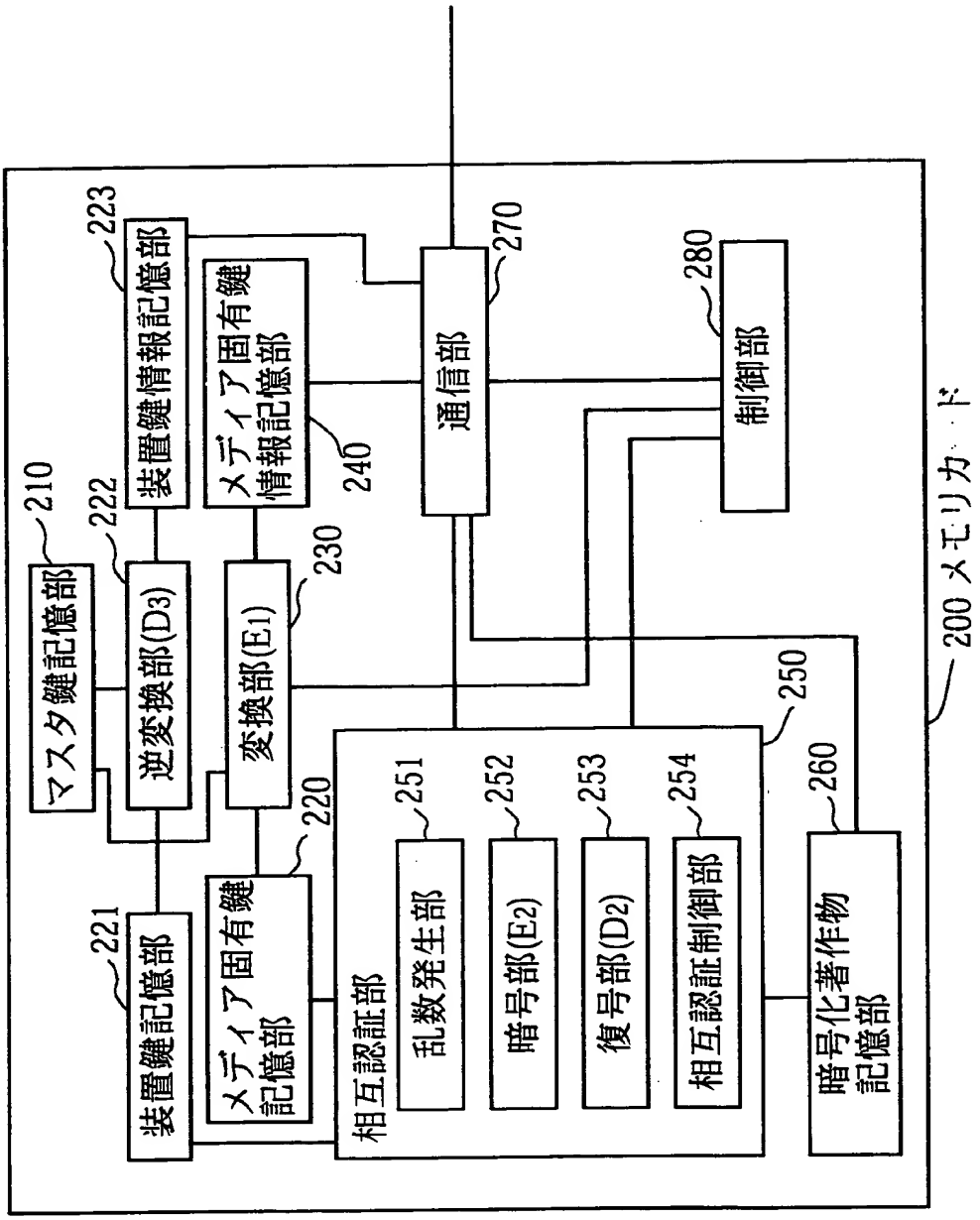
【図２】


ディスプレイ 503
スピーカ 502
通信回線
300
200
メモリカード
301
メモリカード
挿入口
10
メモリカード
ライタ
501
メモリカード
挿入口
スピーカ 502
キーボード 504
パーソナルコンピュータ 500

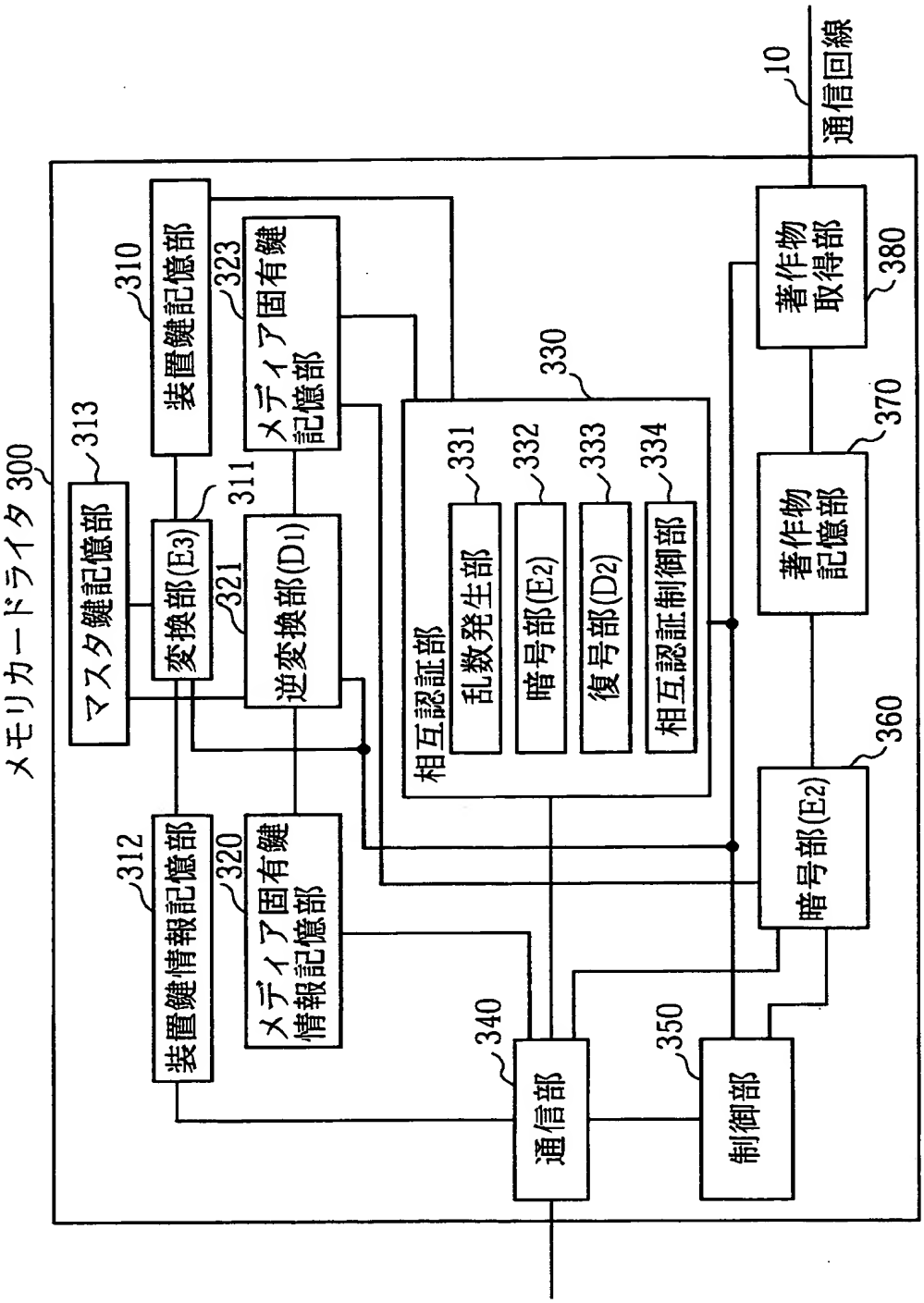
【図３】


ヘッドホン 402
ヘッドホンステレオ 401
404a
404b
404c
404d
403 メモリカード挿入口
200
メモリカード

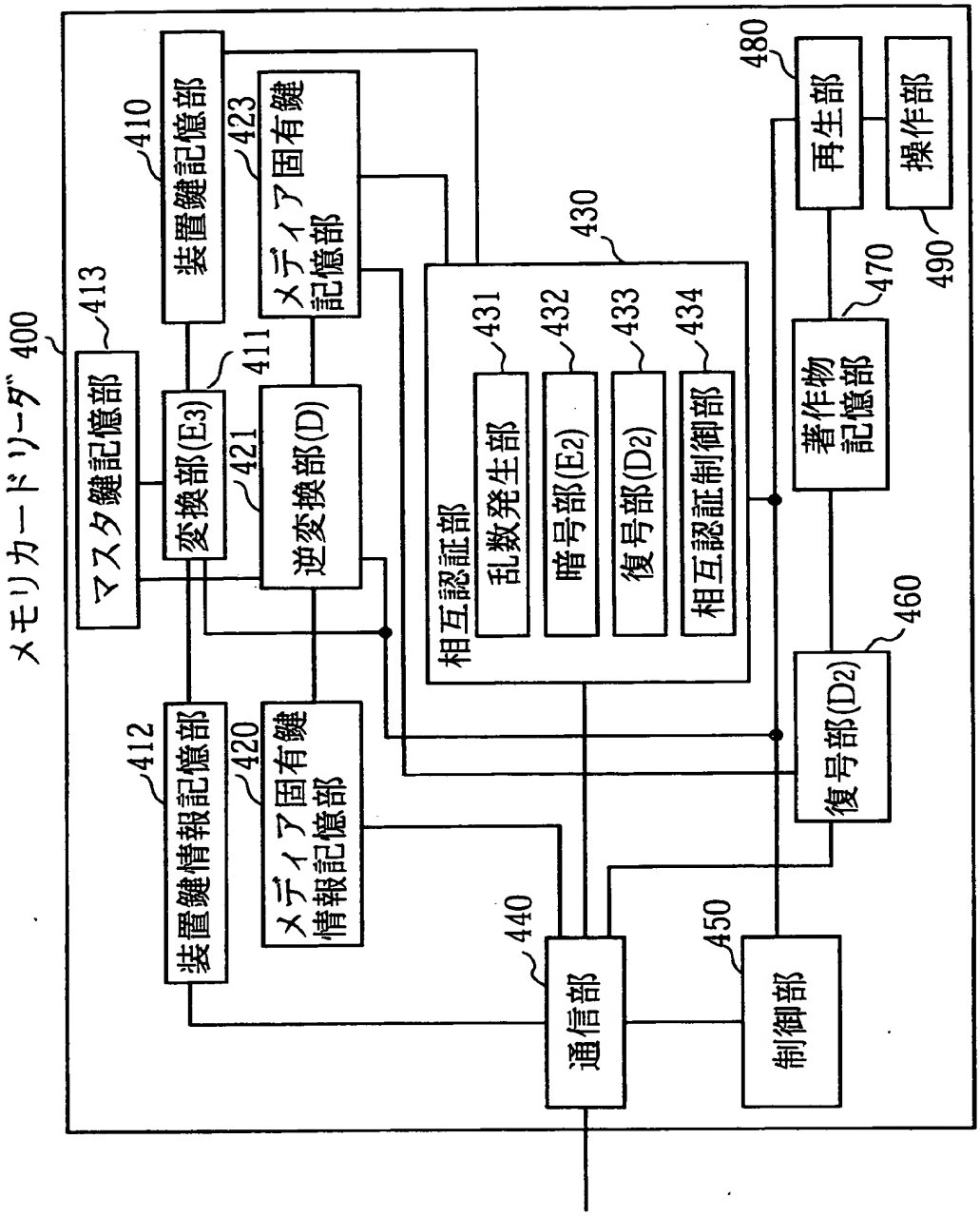
【図４】


200 メモリカード
210 マスタ鍵記憶部
221 装置鍵記憶部
222 逆変換部(D3)
223 装置鍵情報記憶部
220 メディア固有鍵記憶部
230 変換部(E1)
240 メディア固有鍵情報記憶部
250 相互認証部
251 乱数発生部
252 暗号部(E2)
253 復号部(D2)
254 相互認証制御部
260 暗号化著作物記憶部
270 通信部
280 制御部

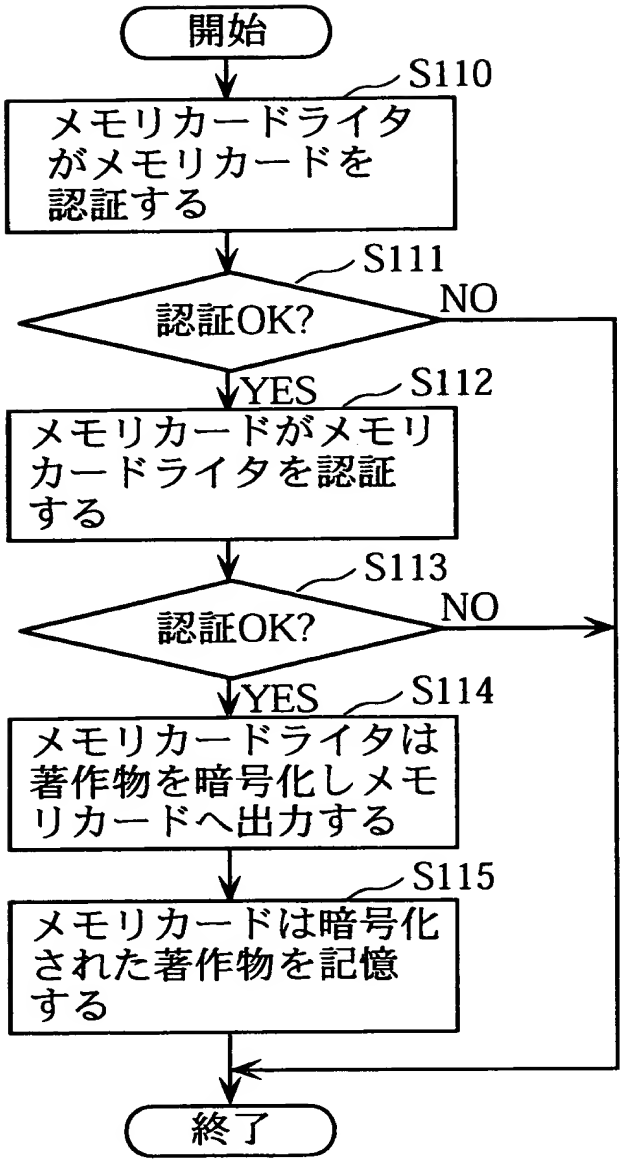
【図５】


メモリカードライタ 300
マスタ鍵記憶部
313
装置鍵記憶部
310
変換部(E3)
311
321
逆変換部(D1)
メディア固有鍵記憶部
323
装置鍵情報記憶部
312
メディア固有鍵情報記憶部
320
相互認証部
330
乱数発生部
331
暗号部(E2)
332
復号部(D2)
333
相互認証制御部
334
通信部
340
制御部
350
暗号部(E2)
360
著作物記憶部
370
著作物取得部
380
10
通信回線

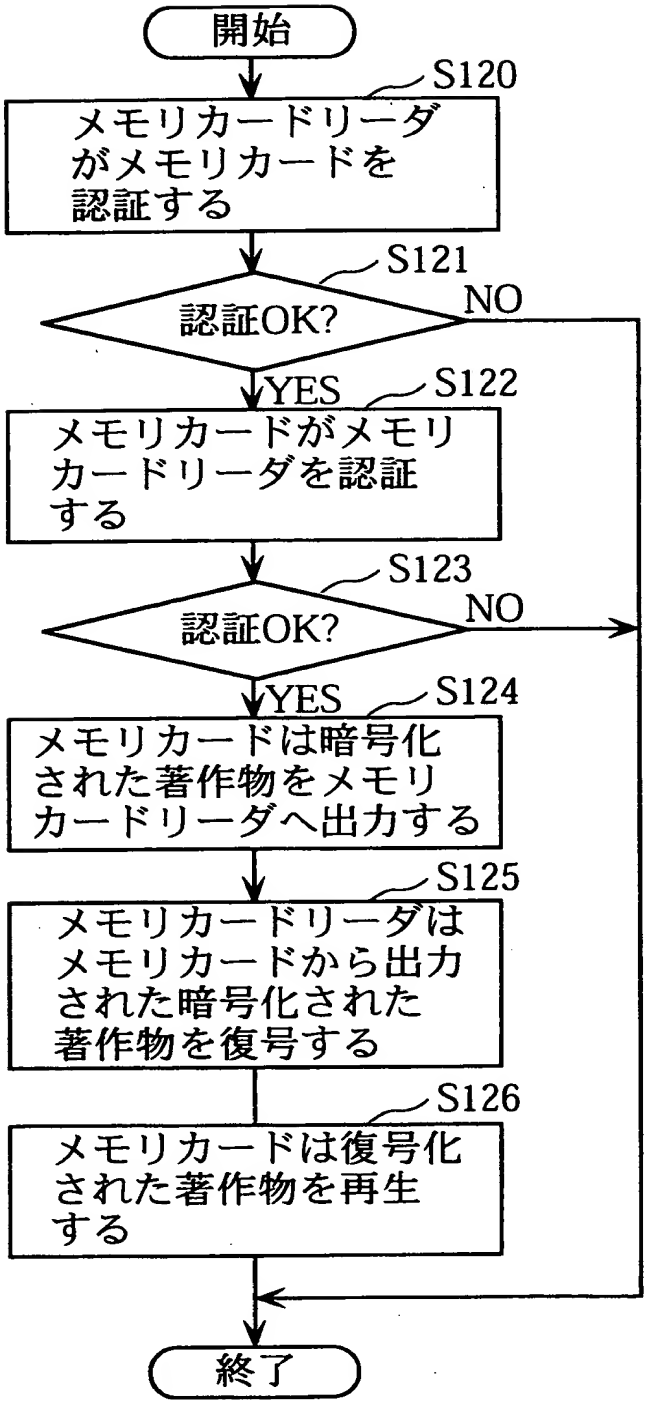
【図６】


メモリカードリーダ" 400
マスタ鍵記憶部 413
装置鍵記憶部 410
変換部(E3) 411
逆変換部(D) 421
メディア固有鍵記憶部 423
装置鍵情報記憶部 412
メディア固有鍵情報記憶部 420
相互認証部 430
乱数発生部 431
暗号部(E2) 432
復号部(D2) 433
相互認証制御部 434
通信部 440
制御部 450
復号部(D2) 460
著作物記憶部 470
再生部 480
操作部 490

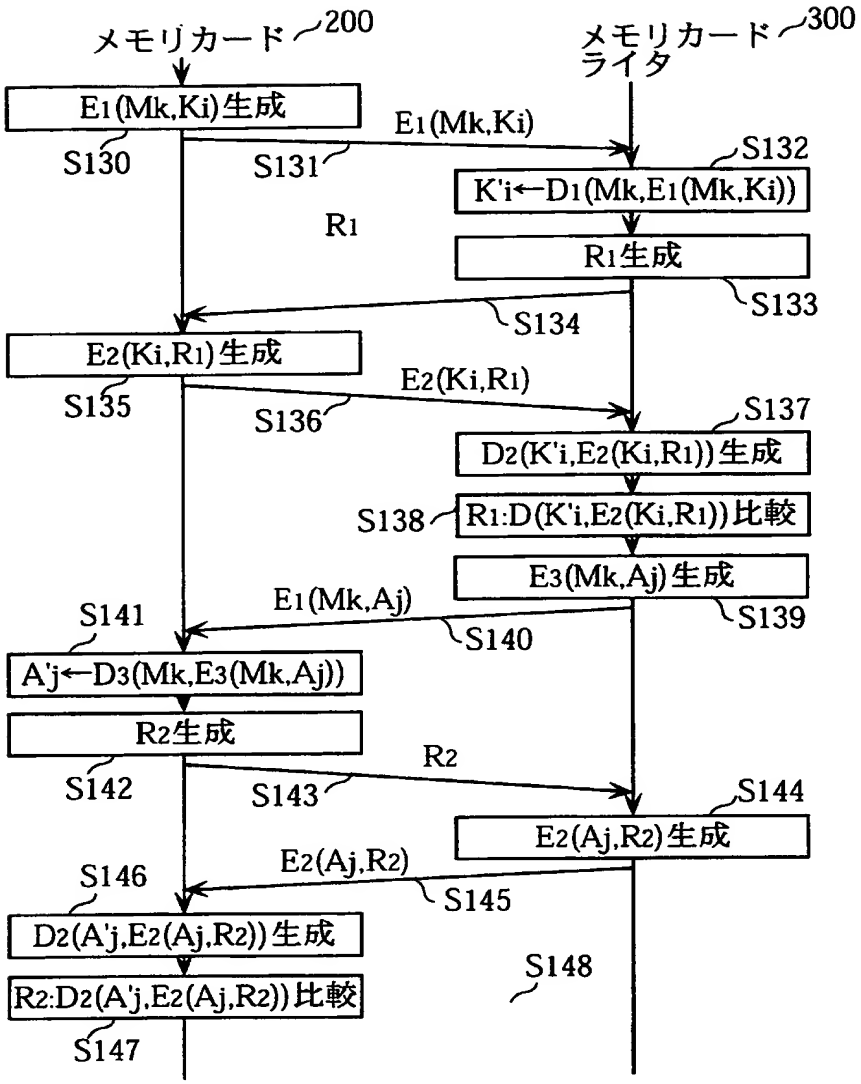
【図７】


開始
S110
メモリカードライタがメモリカードを認証する
S111
認証OK?
NO
YES
S112
メモリカードがメモリカードライタを認証する
S113
認証OK?
NO
YES
S114
メモリカードライタは著作物を暗号化しメモリカードへ出力する
S115
メモリカードは暗号化された著作物を記憶する
終了

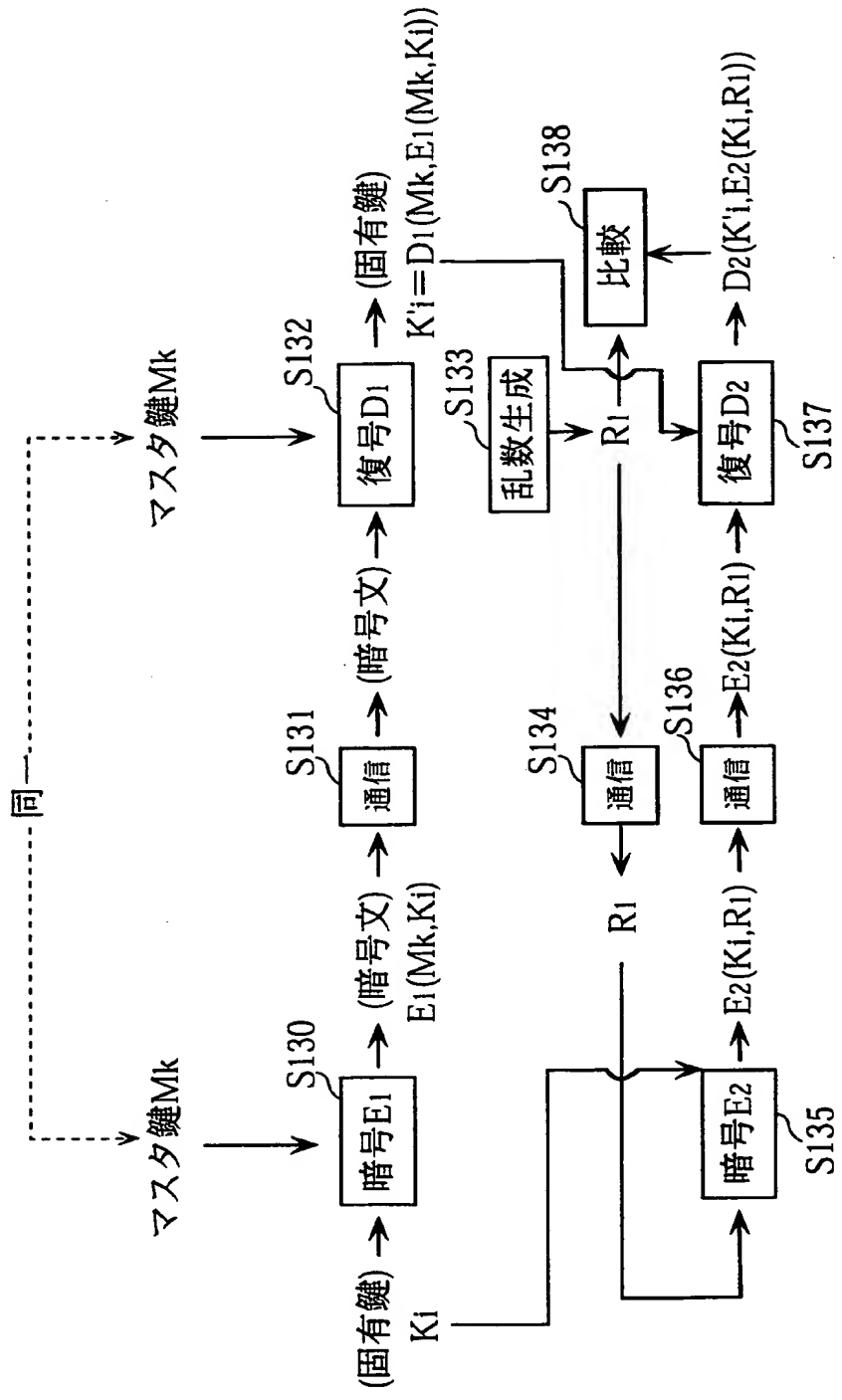
【図８】


開始
S120
メモリカードリーダがメモリカードを認証する
S121
認証OK?
NO
YES
S122
メモリカードがメモリカードリーダを認証する
S123
認証OK?
NO
YES
S124
メモリカードは暗号化された著作物をメモリカードリーダへ出力する
S125
メモリカードリーダはメモリカードから出力された暗号化された著作物を復号する
S126
メモリカードは復号化された著作物を再生する
終了

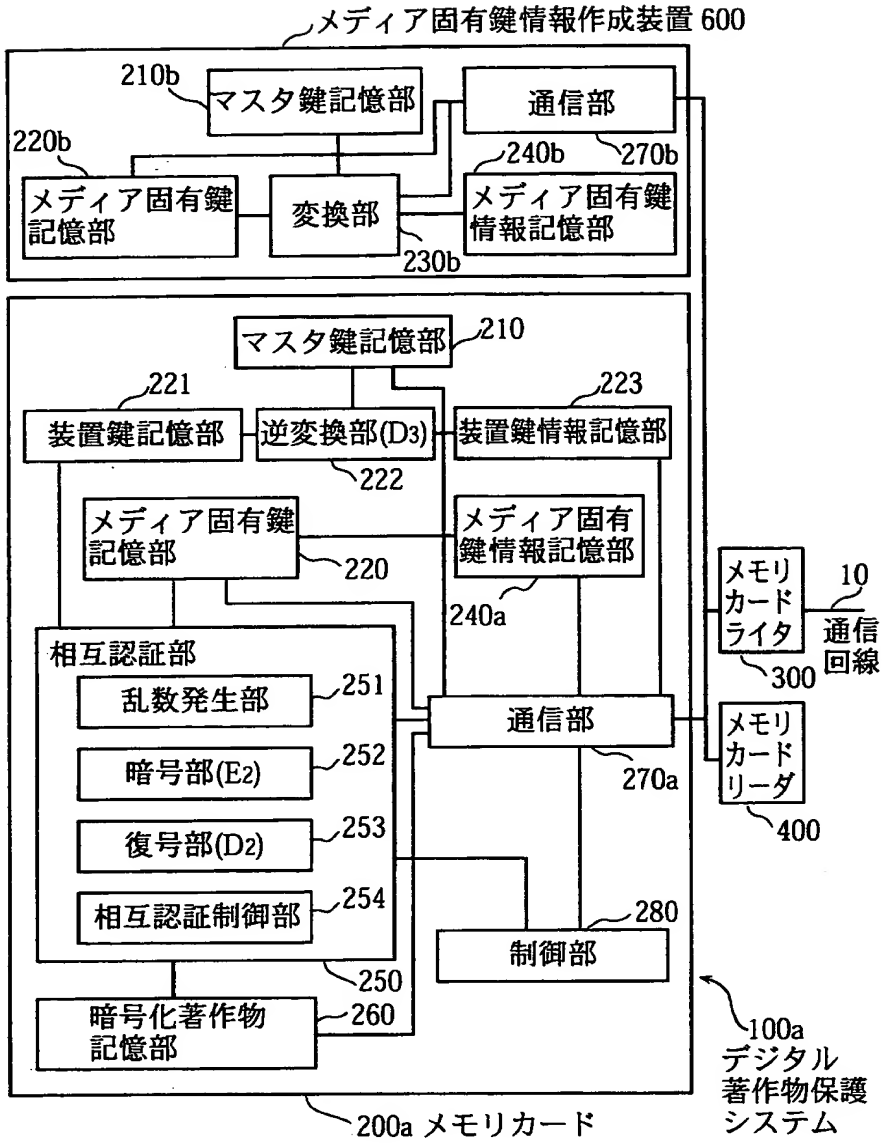
【図９】


メモリカード 200
メモリカード ライタ 300
E1(Mk,Ki)生成
S130
E1(Mk,Ki)
S131
S132
K'i←D1(Mk,E1(Mk,Ki))
R1
R1生成
S133
S134
E2(Ki,R1)生成
S135
E2(Ki,R1)
S136
S137
D2(K'i,E2(Ki,R1))生成
S138
R1:D(K'i,E2(Ki,R1))比較
E3(Mk,Aj)生成
S139
S141
E1(Mk,Aj)
S140
A'j←D3(Mk,E3(Mk,Aj))
R2生成
S142
R2
S143
S144
E2(Aj,R2)生成
S146
E2(Aj,R2)
S145
D2(A'j,E2(Aj,R2))生成
S148
R2:D2(A'j,E2(Aj,R2))比較
S147

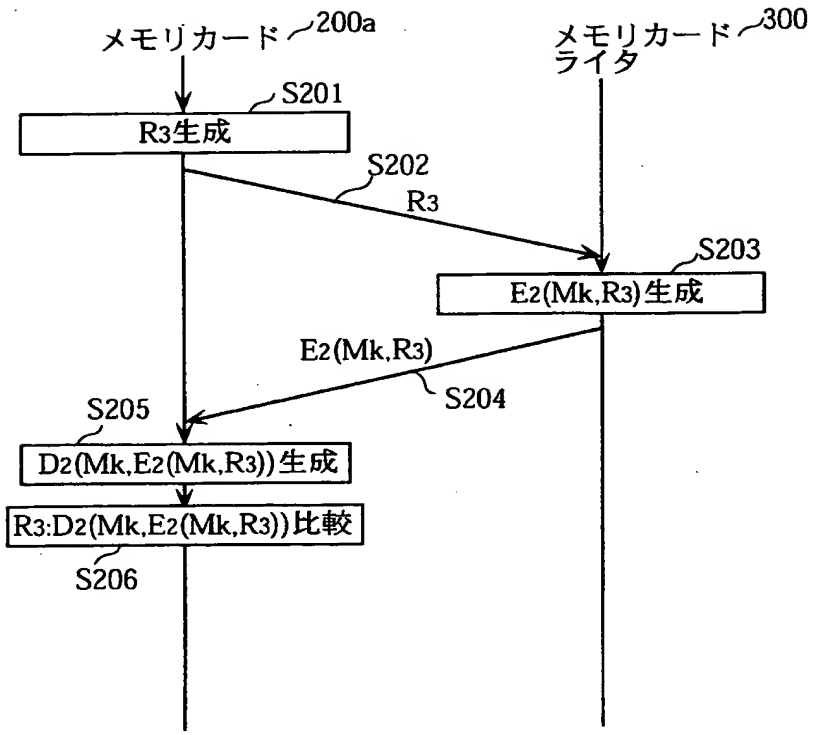
【図１０】


同一
マスタ鍵Mk
マスタ鍵Mk
(固有鍵)
Ki
S130
暗号E1
(暗号文)
E1(Mk,Ki)
S131
通信
(暗号文)
S132
復号D1
(固有鍵)
K'i=D1(Mk,E1(Mk,Ki))
S133
乱数生成
R1
S134
通信
R1
S135
暗号E2
E2(Ki,R1)
S136
通信
E2(Ki,R1)
S137
復号D2
D2(K'i,E2(Ki,R1))
S138
比較

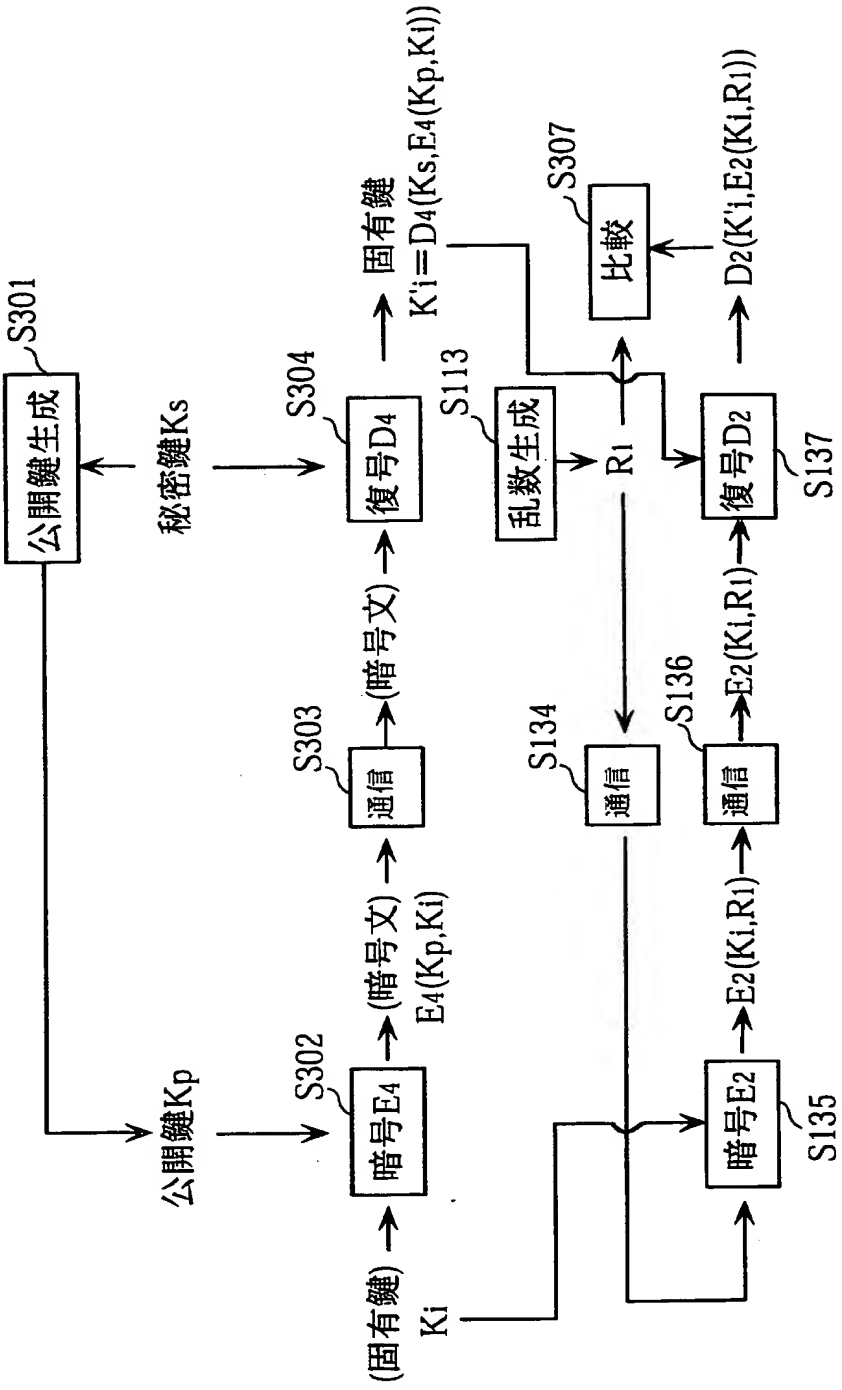
【図１１】


メディア固有鍵情報作成装置 600
210b
マスタ鍵記憶部
通信部
220b
240b
270b
メディア固有鍵記憶部
変換部
メディア固有鍵情報記憶部
230b
マスタ鍵記憶部
210
221
223
装置鍵記憶部
逆変換部(D3)
装置鍵情報記憶部
222
メディア固有鍵記憶部
220
メディア固有鍵情報記憶部
240a
メモリカードライタ
10
通信回線
300
相互認証部
乱数発生部
251
通信部
メモリカードリーダ
暗号部(E2)
252
270a
復号部(D2)
253
400
相互認証制御部
254
280
制御部
250
暗号化著作物記憶部
260
100a
デジタル著作物保護システム
200a メモリカード

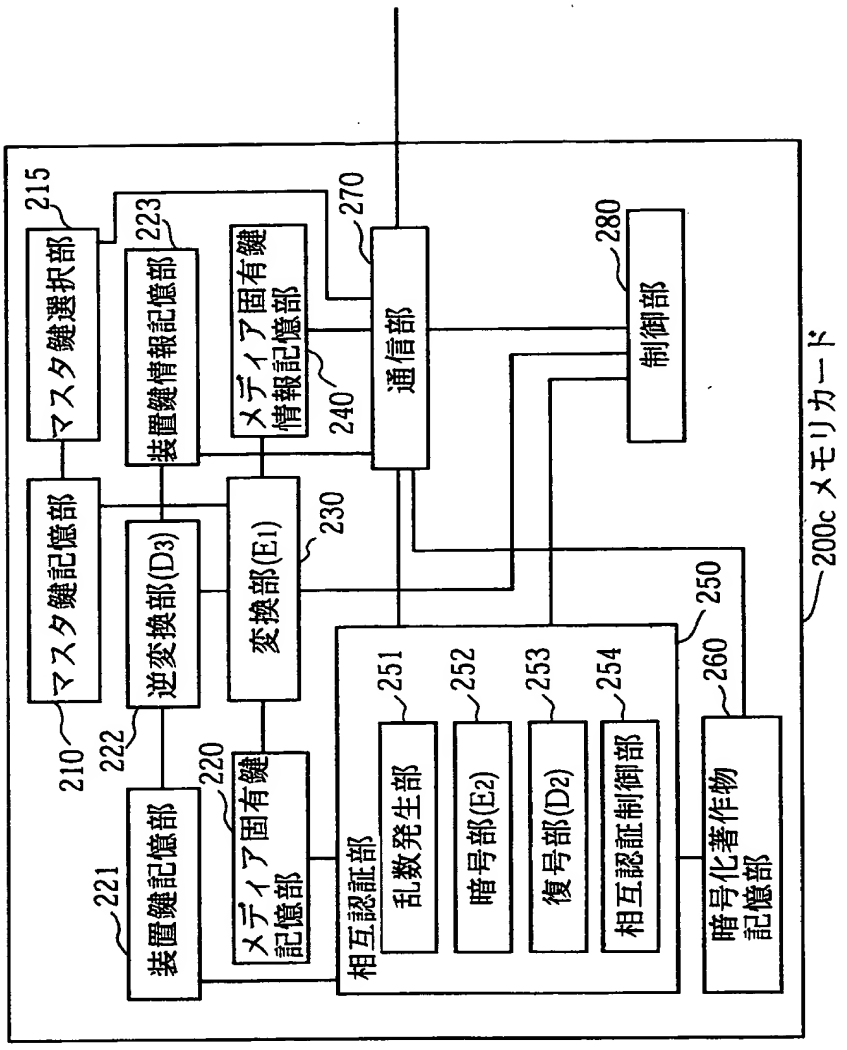
【図１２】


メモリカード
200a
メモリカード
ライタ
300
S201
R3生成
S202
R3
S203
E2(Mk,R3)生成
E2(Mk,R3)
S204
S205
D2(Mk,E2(Mk,R3))生成
R3:D2(Mk,E2(Mk,R3))比較
S206

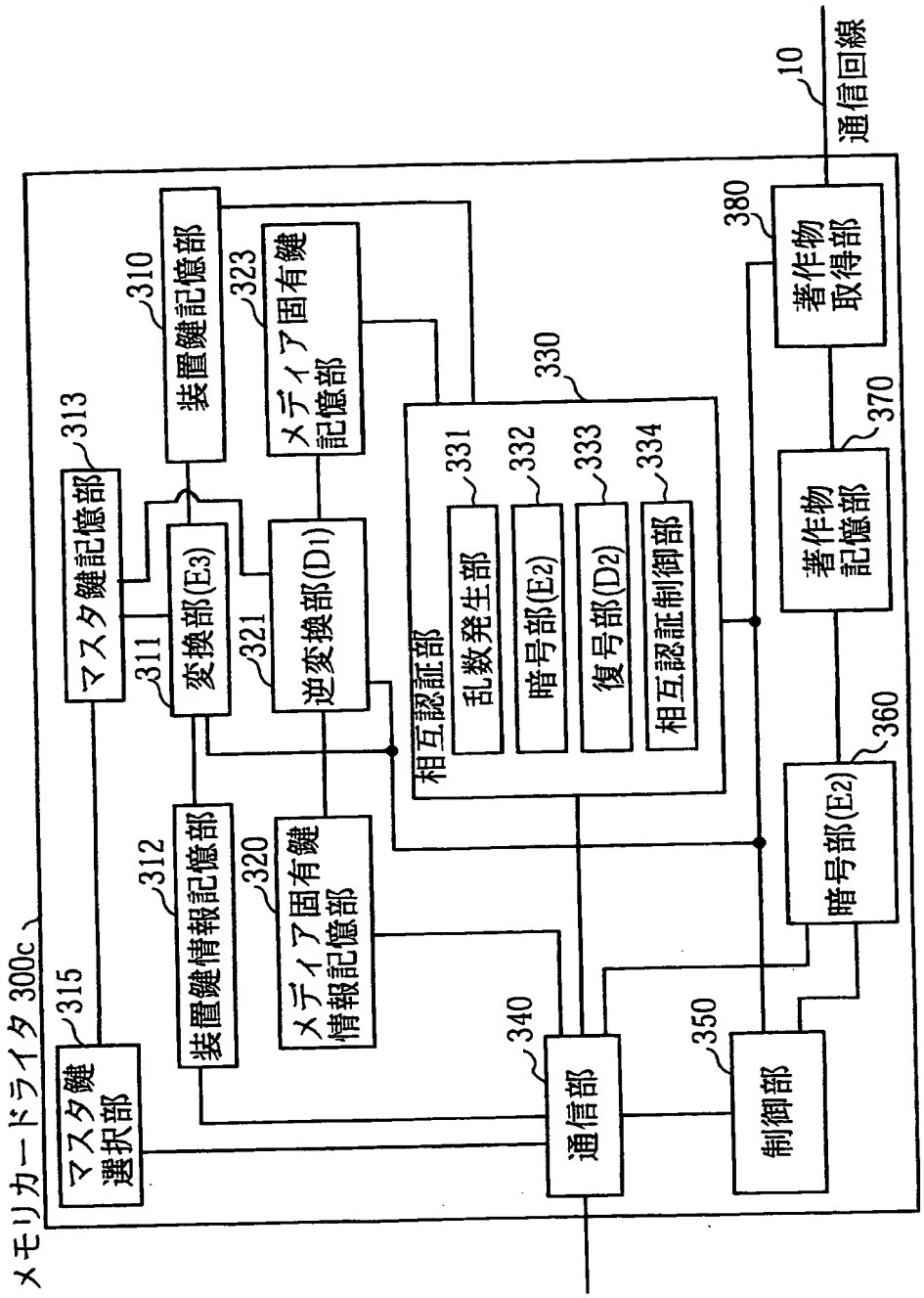
【図１３】


公開鍵生成
S301
秘密鍵Ks
公開鍵Kp
S302
暗号E4
(暗号文)
E4(Kp,Ki)
S303
通信
(暗号文)
S304
復号D4
固有鍵
K'i=D4(Ks,E4(Kp,Ki))
(固有鍵)
Ki
S113
乱数生成
R1
S134
通信
S135
暗号E2
E2(Ki,R1)
S136
通信
E2(Ki,R1)
S137
復号D2
D2(K'i,E2(Ki,R1))
S307
比較

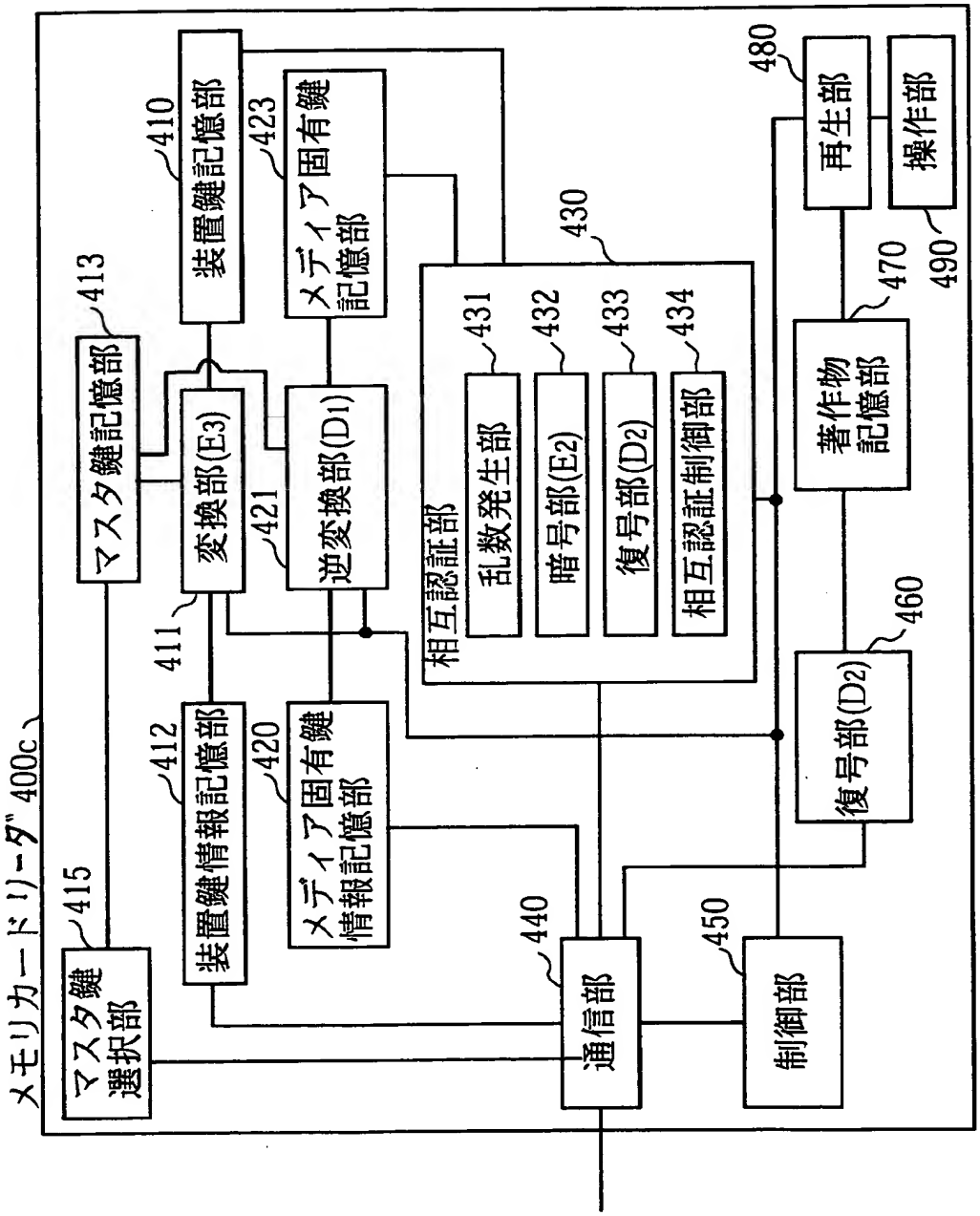
【図１４】


200c メモリカード
マスタ鍵選択部
215
装置鍵情報記憶部
223
メディア固有鍵情報記憶部
240
270
通信部
280
制御部
マスタ鍵記憶部
210
逆変換部(D3)
222
変換部(E1)
230
装置鍵記憶部
221
メディア固有鍵記憶部
220
相互認証部
250
乱数発生部
251
暗号部(E2)
252
復号部(D2)
253
相互認証制御部
254
暗号化著作物記憶部
260

【図１５】


メモリカードライタ 300c
マスタ鍵選択部
315
マスタ鍵記憶部
313
311
装置鍵情報記憶部
312
装置鍵記憶部
310
変換部(E3)
メディア固有鍵情報記憶部
320
メディア固有鍵記憶部
323
逆変換部(D1)
321
相互認証部
330
乱数発生部
331
暗号部(E2)
332
復号部(D2)
333
相互認証制御部
334
通信部
340
制御部
350
暗号部(E2)
360
著作物記憶部
370
著作物取得部
380
10
通信回線

【図１６】


メモリカードリーダ" 400c
マスタ鍵選択部
415
マスタ鍵記憶部
413
装置鍵情報記憶部
412
装置鍵記憶部
410
変換部(E3)
411
メディア固有鍵情報記憶部
420
逆変換部(D1)
421
メディア固有鍵記憶部
423
相互認証部
430
乱数発生部
431
暗号部(E2)
432
復号部(D2)
433
相互認証制御部
434
通信部
440
制御部
450
復号部(D2)
460
著作物記憶部
470
再生部
480
操作部
490

【書類名】　要約書

【要約】

【課題】　外部から取り出したデジタル著作物を不正に記録媒体へ書き込むことと記録媒体に記録されたデジタル著作物を不正に再生することを防止する。

【解決手段】

メディア固有鍵記憶部２２０はあらかじめ一つの固有鍵Ｋｉ を記憶し、変換部２３０は読み出した固有鍵Ｋｉ から暗号化固有鍵Ｊｉ を生成し、乱数発生部２５１は乱数Ｒ2 を生成し、暗号部２５２は乱数Ｒ1 から暗号化乱数Ｓ1 を生成し、復号部２５３は暗号化乱数Ｓ2 から乱数Ｒ’２ を生成し、相互認証制御部２５４は乱数Ｒ’２ と乱数Ｒ2 とを比較し一致すればメモリカード２００が装着されたメモリカードライタ、メモリカードリーダが正しい装置と認証する。

【選択図】　図４

【書類名】　職権訂正データ
【訂正書類】　特許願

＜認定情報・付加情報＞
【特許出願人】
【識別番号】　000005821
【住所又は居所】　大阪府門真市大字門真１００６番地
【氏名又は名称】　松下電器産業株式会社
【代理人】　申請人
【識別番号】　100090446
【住所又は居所】　大阪市北区豊崎３丁目２番１号　淀川５番館６Ｆ
中島国際特許事務所
【氏名又は名称】　中島　司朗
【代理人】
【識別番号】　100109210
【住所又は居所】　大阪市北区豊崎３丁目２番１号　淀川５番館６Ｆ
中島国際特許事務所
【氏名又は名称】　新居　広守

出　願　人　履　歴　情　報

識別番号　　〔０００００５８２１〕

１．変更年月日　　１９９０年　８月２８日
［変更理由］　新規登録
住　所　　大阪府門真市大字門真１００６番地
氏　名　　松下電器産業株式会社